University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25th May, 2021
Zhewen Zheng

Homework 1

Problems to TURN IN

1. Read the ”symmetries of the tetrahedron” supplement in the content for lecture 1 on canvas. Adopt the notation of figure 1.4 in supplement. Show that the axis of the composite rotation srs passes through the vertex labeled 4, and that the axis of $rsrr$ is determined by the midpoints of the line segment edges [12] and [34]. (You can build your own tetrahedron using the pattern provided in the content for lecture 1 on canvas.)

   Solution:

   First,

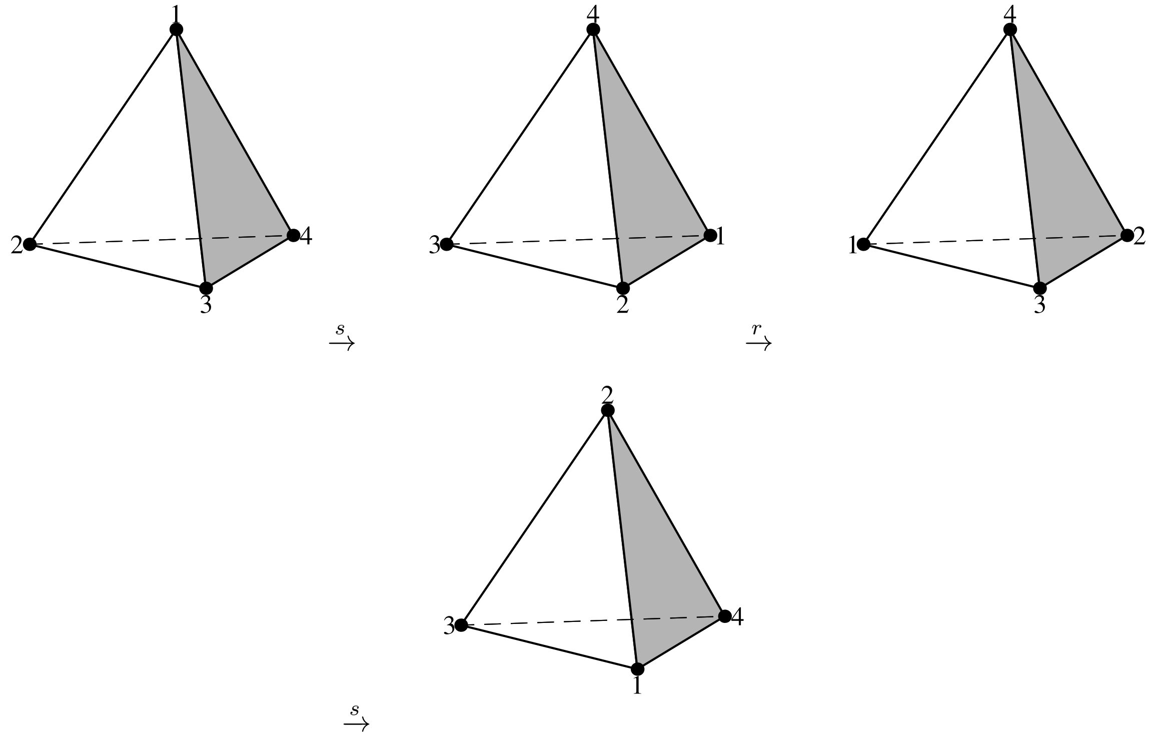

Figure 1: srs

As we can see, rotate the original through the axis through vertex labeled 4 produces the same result as the composite rotation srs.

Next,

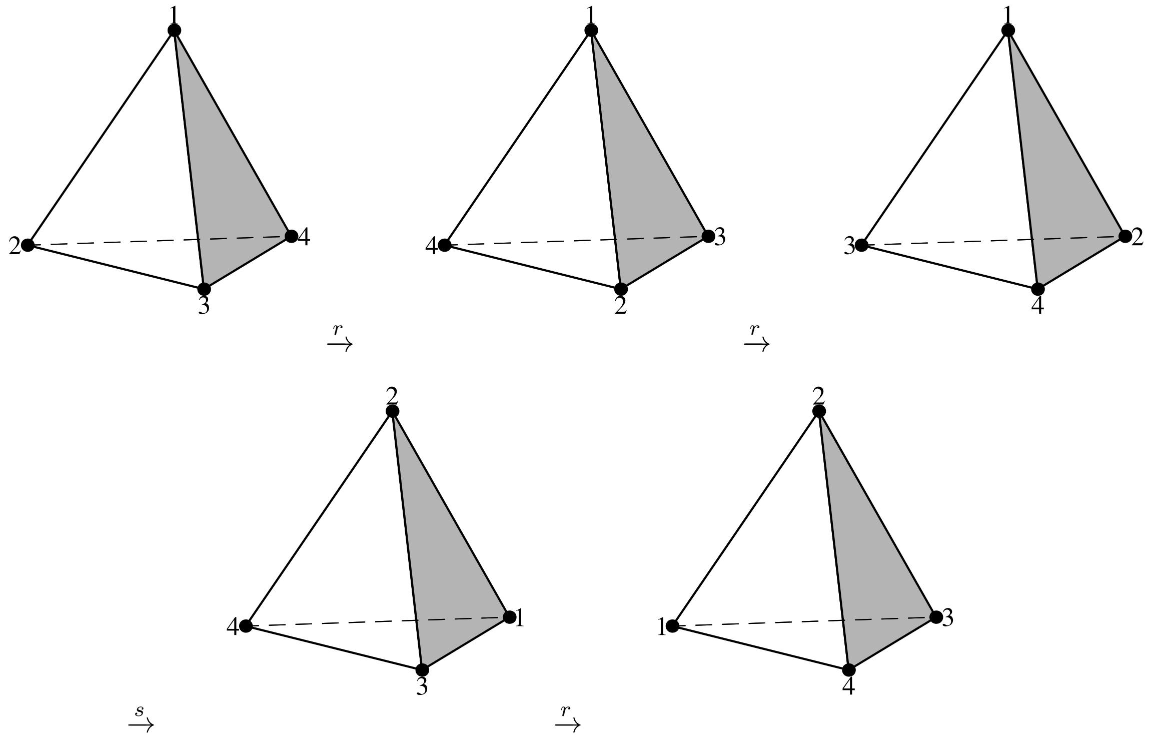

Figure 2: $rsrr$

As we see rotate the original by the midpoints of the line segment edges [12] and [34] gives the same result.

2. Having completed the previous exercise, express each of the twelve rotational symmetries of the tetrahedron in terms of r and s.

   Solution:

$$e, r, r^2, s, rs, r^2s, sr, rsr, r^2sr, sr^2, rsr^2, r^2sr^2$$

3. p.180:4
   Determine whether the set G is a group under the operation $*$.

   (a) $G = \{2, 4, 6, 8\}$ in $\mathbb{Z}_{10}; a * b = ab$

   Solution:

- Closure:

$\cdot$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

- Associativity: $(a * b) * c = (ab)c = a(bc) = a * (b * c)$
- Identity: $e = 6$,see the Cayley Table
- Inverse: Exists for all $a \in G$. See the Cayley table. Thus G is a group under $*$.

(b) $G = \mathbb{Z}; a * b = a - b$

Solution:

- Closure: For all $a, b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$.
- Associativity: $(a - b) - c \neq a - (b - c)$. Thus G is not a group under $*$.

(c) $G = \{n \in \mathbb{Z} \mid n \text{ is odd}\}; a * b = a + b$

Solution:

- Closure: $a, -a \in G, a * (-a) = a + (-a) = 0 \notin G$. Thus G is not a group under $*$.

(d) $G = \{2^x \mid x \in \mathbb{Q}\}; a * b = ab$

Solution:

- Closure: Let $a = 2^x, b = 2^y, x, y \in \mathbb{Q}; a * b = ab = 2^{x+y}, x + y \in \mathbb{Q}$.
- Associativity: $(a * b) * c = (ab)c = (2^x 2^y)2^z = 2^x(2^y 2^z) = a(bc) = a * (b * c)$
- Identity: $a * e = 2^x \cdot 1 = 2^x 2^0; e = 2^0, 0 \in \mathbb{Q}$
- Inverse: $a * a^{-1} = 2^x 2^{-x} = 2^0 = 1 = e$. Thus G is a group under $*$.

4. p.181:7.

(a) Show that the group $GL(2, \mathbb{Z}_2)$ has order 6 by listing all its elements.

Solution:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

(b) Show by example that the groups $GL(2, \mathbb{R})$ and $GL(2, \mathbb{Z}_2)$ are nonabelian.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$
$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ea + fc & eb + fd \\ ga + hc & gb + hd \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \neq \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

(c) Additionally show that $GL(2, \mathbb{F}_2)$ is isomorphic to S_3.

Solution:

S_3	123	132	213	231	312	321	$\cdot$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
123	123	132	213	231	312	321	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
132	132	123	312	321	213	231	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$
213	213	231	123	132	321	312	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$
231	231	213	321	312	123	132	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$
312	312	321	132	123	231	213	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$
321	321	312	231	213	132	123	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto 123$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \mapsto 132$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto 213$$
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto 231$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto 312$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto 321$$

5. Let $G = \mathbb{Q} - \{2\}$ and define this operation on G: $a * b = ab - 2a - 2b + 6$ where the operations on the right side of the equal sign are the usual addition and multiplication in $\mathbb{Q}$. Show G is an abelian group. What is the identity? Find a formula for the inverse of a? What is the inverse of $\frac{3}{2}$?

Solution:

(a) Closure: $\mathbb{Q}$ is closed under addition. Check $a * b \neq 2$: Assume that $a * b = 2$

$$\begin{aligned} a * b &= 2 \\ ab - 2a - 2b + 6 &= 2 \\ (a-2)(b-2) + 2 &= 2 \\ (a-2)(b-2) &= 2 \end{aligned}$$

$a = 2$ or $b = 2$. Contradiction to $G = \mathbb{Q} - \{2\}$. Thus G is closed.

(b) Associativity:

$$\begin{aligned} (a * b) * c &= (ab - 2a - 2b + 6)c - 2(ab - 2a - 2b + 6) - 2c + 6 \\ &= abc - 2ac - 2bc + 6c - 2ab + 4a + 4b - 12 - 2c + 6 \\ &= abc - 2ab - 2ac + 6a - 2a - 2bc + 4b + 4c - 12 + 6 \\ &= a(bc - 2b - 2c + 6) - 2a - 2(bc - 2b - 2c + 6) + 6 \\ &= a * (b * c) \end{aligned}$$

(c) Identity:

$$\begin{aligned} a * e &= ae - 2a - 2e + 6 \\ a &= ae - 2a - 2e + 6 \\ 3a &= (a-2)e + 6 \\ 3a - 6 &= (a-2)e \\ e &= 3 \end{aligned}$$

(d) Inverse:

$$\begin{aligned} a * a^{-1} &= aa^{-1} - 2a - 2a^{-1} + 6 \\ 3 &= aa^{-1} - 2a - 2a^{-1} + 6 \\ 3 &= (a-2)a^{-1} - 2(a-2) + 2 \\ 3 &= (a-2)(a^{-1} - 2) + 2 \\ \frac{1}{a-2} &= a^{-1} - 2 \\ a^{-1} &= \frac{2a-3}{a-2} \end{aligned}$$

(e) Inverse of $\frac{3}{2}$

$$\begin{aligned} \frac{3}{2}^{-1} &= \frac{3-3}{\frac{3}{2} - 2} \\ &= 0 \end{aligned}$$

6. p.182:28
Prove that each element of a finite group G appears exactly once in each row and exactly once in each column of the operation table.

Solution:

Assume an element of a finite group G appears more than once in each row. Then

$$\begin{aligned} ab &= ac, b \neq c \\ a^{-1}ab &= a^{-1}ac \\ eb &= ec \\ b &= c \end{aligned}$$

Contradiction. Similarly for columns:

$$\begin{aligned} ab &= cb, a \neq c \\ abb^{-1} &= cbb^{-1} \\ ae &= ce \\ a &= c \end{aligned}$$

Contradiction. Thus an element of a finite group G cannot appear more than once in each row nor in each column. Since G is a group, G is closed, an element of G must appear at least once (multiply by identity). There fore each element of a finite group G appears exactly once in each row and exactly once in each column of the operation.

7. For each of the follow groups, list all of the elements, compute the order of each element, then construct an isomorphism with either $\mathbb{Z}_n$ (for some n) or a finite product of $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$: (a) $\mathbb{U}_8$; (b) $\mathbb{U}_{11}$; (c) $\mathbb{U}_{27}$; (d) $\mathbb{U}_{36}$.

Solution:

(a) $\mathbb{U}_8 = \{1, 3, 5, 7\}$

$$|1| = 1, |3| = 2, |5| = 2.|7| = 2$$

Let $H = \langle 3 \rangle, K = \langle 5 \rangle, H \times K = \{(1, 1), (1, 3), (1, 5), (3, 5)\}$.
$\phi : H \times K \to \mathbb{U}_8$ where $\phi(a, b) = ab$.

$$\begin{aligned} \phi((a, b)(c, d)) &= \phi(ac, bd) \\ &= acbd \\ &= abcd \\ &= \phi(a, b)\phi(c, d) \end{aligned}$$

Since $H \times K$ and $\mathbb{U}_8$ are finite, this is an isomorphism. Notice that H is isomorphic to $\mathbb{Z}_2$, K is isomorphic to $\mathbb{Z}_2$. Thus $\mathbb{U}_8 \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

(b) $\mathbb{U}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$|1| = 1, |2| = 10, |3| = 5, |4| = 5, |5| = 5, |6| = 10, |7| = 10, |8| = 10, |9| = 5, |10| = 2$$

Notice $\mathbb{U}_{11} = \langle 2 \rangle$. Thus $\mathbb{U}_{11} \cong \langle 2 \rangle \cong \mathbb{Z}_{10}$

(c) $\mathbb{U}_{27} = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$

$$|1| = 1, |2| = 18, |4| = 9, |5| = 18, |7| = 9, |8| = 6, |10| = 3, |11| = 18, |13| = 9,$$
$$|14| = 18, |16| = 9, |17| = 6, |19| = 3, |20| = 18, |22| = 9, |23| = 18, |25| = 9, |26| = 2$$

Notice that $|\mathbb{U}_{27}| = 18$ and $|2| = 18$. We have $\mathbb{U}_{27} = \langle 2 \rangle$. By Theorem 7.19, $\langle 2 \rangle \cong \mathbb{Z}_{18}$. Thus $\mathbb{U}_{27} \cong \mathbb{Z}_{18}$.

(d) $\mathbb{U}_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$

$$|1| = 1, |5| = 6, |7| = 6, |11| = 6, |13| = 3, |17| = 2, |19| = 2,$$
$$|23| = 6, |25| = 3, |29| = 6, |31| = 6, |35| = 2$$

Consider $H = \langle 5 \rangle = \{1, 5, 25, 17, 13, 29\}$ and $K = \langle 35 \rangle = \{1, 35\}$. We can easily verify that G is the internal direct product $H \times K$. Thus $G \cong H \times K$. Now, notice that $|H| = 6, |K| = 2$ and by Theorem 7.19, $H \cong \mathbb{Z}_6, K \cong \mathbb{Z}_2$. Therefore $\mathbb{U}_{36} \cong H \times K \cong \mathbb{Z}_6 \times \mathbb{Z}_2$.

8. This problem works on the unit circle $\mathbb{T}$ in the plane; i.e. the points (x, y) in the plane satisfying the equation $x^2 + y^2 = 1$. A point $(\alpha, \beta) \in \mathbb{T}$ is called a rational point if $\alpha, \beta \in \mathbb{Q}$. Given rational points (α, β) and (γ, λ) on the unit circle, define an operation $\star$

$$(\alpha, \beta) \star (\gamma, \lambda) = (\alpha\gamma - \beta\lambda, \alpha\lambda + \beta\gamma)$$

(a) Show the set $\mathbb{T}_Q$ of rational points on the unit circle is a group under the operation $\star$.

Solution:

i. Well-defined:

$$\begin{aligned}(\alpha, \beta) * (\gamma, \lambda) &= (\alpha\gamma - \beta\lambda, \alpha\lambda + \beta\gamma) \\ (\alpha\gamma - \beta\lambda)^2 + (\alpha\lambda + \beta\gamma)^2 &= \alpha^2\gamma^2 - 2\alpha\gamma\beta\lambda + \beta^2\lambda^2 + \alpha^2\lambda^2 + 2\alpha\lambda\beta\gamma + \beta^2\gamma^2 \\ &= \alpha^2\gamma^2 + \beta^2\lambda^2 + \alpha^2\lambda^2 + \beta^2\gamma^2 \\ &= \alpha^2(\gamma^2 + \lambda^2 + \beta^2(\lambda^2 + \gamma^2) \\ &= \alpha^2 + \beta^2 \\ &= 1\end{aligned}$$

ii. Closure:

$$(\alpha, \beta) * (\gamma, \lambda) = (\alpha\gamma - \beta\lambda, \alpha\lambda + \beta\gamma)$$

where $\alpha\gamma - \beta\lambda, \alpha\lambda + \beta\gamma \in \mathbb{Q}$.

iii. Associativity:

$$\begin{aligned}((\alpha, \beta) * (\gamma, \lambda)) * (\eta, \theta) &= (\alpha\gamma - \beta\lambda, \alpha\lambda + \beta\gamma) * (\eta, \theta) \\ &= ((\alpha\gamma - \beta\lambda)\eta - (\alpha\lambda + \beta\gamma)\theta, (\alpha\gamma - \beta\lambda)\theta + (\alpha\lambda + \beta\gamma)\eta) \\ &= (\alpha(\gamma\eta - \lambda\theta) - \beta(\gamma\theta + \lambda\eta), \alpha(\gamma\theta + \lambda\eta) + \beta(\gamma\eta - \lambda\theta)) \\ &= (\alpha, \beta) * (\gamma\eta - \lambda\theta, \gamma\theta + \lambda\eta) \\ &= (\alpha, \beta) * ((\gamma, \lambda) * (\eta, \theta))\end{aligned}$$

iv. Identity:

$$\begin{aligned}(\alpha, \beta) * (e_1, e_2) &= (\alpha e_1 - \beta e_2, \alpha e_2 + \beta e_1)\\ &= (\alpha, \beta)\\ (e_1, e_2) &= (1, 0)\end{aligned}$$

v. Inverse:

$$\begin{aligned}(\alpha, \beta) * (\alpha, \beta)^{-1} &= (1, 0)\\ (\alpha, \beta)^{-1} &= (\alpha, -\beta)\end{aligned}$$

(b) Calculate $(\frac{15}{17}, \frac{8}{17}) \star (\frac{4}{5}, \frac{3}{5})$

Solution:

$$\begin{aligned}\left(\frac{15}{17}, \frac{8}{17}\right) \star \left(\frac{4}{5}, \frac{3}{5}\right) &= \left(\frac{15}{17}\frac{4}{5} - \frac{8}{17}\frac{3}{5}, \frac{15}{17}\frac{3}{5} + \frac{8}{17}\frac{4}{5}\right)\\ &= \left(\frac{36}{85}, \frac{77}{85}\right)\end{aligned}$$

(c) If $m \in \mathbb{Q}$, define $P_m = (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$. Show $P_m \in \mathbb{T}_Q$. Convince yourself that $\mathbb{T}_Q$ is a dense subset of $\mathbb{T}$. (Look up the definition of a dense set if you are unfamiliar with this terminology.)

Solution:

$$\begin{aligned}\left(\frac{1-m^2}{1+m^2}\right)^2 + \left(\frac{2m}{1+m^2}\right)^2 &= \frac{(1-m^2)^2 + (2m)^2}{(1+m)^2}\\ &= \frac{1+2m^2+4m^2}{(1+m^2)^2}\\ &= \frac{(1+m^2)^2}{(1+m^2)^2}\\ &= 1\end{aligned}$$

It is clear that $(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}) \in \mathbb{T}_Q$, since the above and

$$\frac{1-m^2}{1+m^2} \in \mathbb{Q}, \frac{2m}{1+m^2} \in \mathbb{Q},$$

(d) Give an example of an element in $\mathbb{T}_Q$ of finite order. Give an example of an element in $\mathbb{T}_Q$ of infinite order.

Solution:

Element of finite order:

$$|(0,1)| = 4, (0,1)^4 = (1,0)$$

Element of infinite order:

$$\left|\left(\frac{3}{5}, \frac{4}{5}\right)\right| = \infty$$

To verify, use part (e) below: consider $(\alpha, \beta) = (\cos\theta, \sin\theta)$. Clearly by the trigonometric identities, the element has finite order only when $\theta = k\pi$ when $k \in \mathbb{Q}$ (you can always find a big enough integer n to make θ be a even multiple of π as long as θ is a rational multiple of π). Any $a \in \mathbb{Q}$ where $a \neq 0, a \leq 1$ is not a rational multiple of π, thus having infinite order.

(e) Describe the operation $\star$ in terms of geometry of the unit circle.

Solution:

Consider $x = \cos\theta, y = \sin(\theta)$ where θ is the angle the point (x, y) with respect to the positive x-axis. Now

$$\begin{aligned}(\cos\theta, \sin\theta) * (\cos\phi, \sin\phi) &= (\cos\theta\cos\phi - \sin\theta\sin\phi, \cos\theta\sin\phi + \sin\theta\cos\phi) \\ &= (\cos(\theta+\phi), \sin(\theta+\phi))\end{aligned}$$

Essentially, the $\star$ operation sums the angle of two points on the unit circle.

9. (a) Prove: If G is a finite group of order n and $a \in G$, then $|a| \leq n$. In particular, this shows: If G is a finite group, then every element has finite order.

Solution:

Proof. Let G be a finite group of order n, $a \in G$. Suppose $|a| > n$. It cannot be the case that a^k is different for all k. Hence there exists positive s, t such that $a^s = a^t, s < t$. By the well-ordering we can always find a least pair s, t where $a^s = a^t$. If $s > n$, then there must exists at least s different element in G. This is a contradiction as $|G| = n$. Hence $s \leq n$ and $|a| \leq n$. □

(b) Prove: If G is a finite group of order n and $a \in G$, then $|a|$ divides n. In particular, a finite group of odd order cannot contain an element of order 2.

Solution:

Proof. Let G be a finite group of order n, H a subgroup of G, $a \in G$. By Lagrange's Theorem, $|H| \mid |G|$. We know that $\langle a \rangle$ is a subgroup of G (G is closed, $a \in G$, thus for all $k \in \mathbb{Z}$, a^k also in G). By Theorem 7.15, we know that $|\langle a \rangle| = |a|$. Thus $|a| \mid |G| = n$. □

(c) The converse of (a) can fail. Consider the set $\mathbb{S} = \{\cos(\alpha\pi) + i\sin(\alpha\pi) | \alpha \in \mathbb{Q}\}$. Show that $\mathbb{S}$ is an infinite abelian subgroup of the multiplicative group of non-zero complex numbers $\mathbb{C}^\times$. Show every element of $\mathbb{S}$ has finite order.

Solution:

Proof. Let $\mathbb{S} = \{\cos(\alpha\pi)+i\sin(\alpha\pi) \mid \alpha \in \mathbb{Q}\}, \cos(\alpha\pi)+i\sin(\alpha\pi), \cos(\beta\pi)+i\sin(\beta\pi) \in \mathbb{S}$.

i. Closure:

$$\begin{aligned}(\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\beta\pi) + i\sin(\beta\pi)) &= \cos(\alpha\pi)\cos(\beta\pi) - \sin(\alpha\pi)\sin(\beta\pi)\\ &\quad + i(\sin(\alpha\pi)\cos(\beta\pi) + \cos(\alpha\pi)\sin(\beta\pi))\\ &= \cos((\alpha+\beta)\pi) + i\sin((\alpha+\beta)\pi) \neq 0\end{aligned}$$

Never zero because that would require α to be both even and odd.

ii. Associativity:

$$\begin{aligned}&((\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\beta\pi) + i\sin(\beta\pi)))(\cos(\gamma\pi) + i\sin(\gamma\pi))\\ =&(\cos((\alpha+\beta)\pi) + i\sin((\alpha+\beta)\pi))(\cos(\gamma\pi) + i\sin(\gamma\pi))\\ =&\ \cos((\alpha+\beta+\gamma)\pi) + i\sin((\alpha+\beta+\gamma)\pi)\\ =&(\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\beta+\gamma\pi) + i\sin(\beta+\gamma\pi))\\ =&(\cos(\alpha\pi) + i\sin(\alpha\pi))((\cos(\beta\pi) + i\sin(\beta\pi))(\cos(\gamma\pi) + i\sin(\gamma\pi)))\end{aligned}$$

iii. Identity:

$$\begin{aligned}e &= (1,0)\\ &= \cos(0\pi) + i\sin(0\pi)\\ (\cos(\alpha\pi) + i\sin(\alpha\pi))e &= \cos(\alpha\pi + 2\pi) + i\sin(\alpha\pi + 2\pi)\\ &= \cos(\alpha\pi) + i\sin(\alpha\pi)\end{aligned}$$

iv. Inverse:

$$\begin{aligned}(\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\alpha\pi) + i\sin(\alpha\pi))^{-1} &= e\\ (\cos(\alpha\pi) + i\sin(\alpha\pi))^{-1} &= (\cos(\beta\pi) + i\sin(\beta\pi))\\ (\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\beta\pi) + i\sin(\beta\pi)) &= \cos((\alpha+\beta)\pi) + i\sin((\alpha+\beta)\pi)\\ \cos(\beta\pi) + i\sin(\beta\pi) &= \cos(-\alpha\pi) + i\sin(-\alpha\pi)\\ &= \cos(\alpha\pi) - i\sin(\alpha\pi)\end{aligned}$$

v. Commutativity:

$$\begin{aligned}&\cos(\alpha\pi) + i\sin(\alpha\pi))(\cos(\beta\pi) + i\sin(\beta\pi))\\ =&\ \cos((\alpha+\beta)\pi) + i\sin((\alpha+\beta)\pi)\\ =&\ \cos((\beta+\alpha)\pi) + i\sin((\beta+\alpha)\pi)\\ =&\ \cos(\beta\pi) + i\sin(\beta\pi))(\cos(\alpha\pi) + i\sin(\alpha\pi))\end{aligned}$$

vi. Subgroup: See above. $\forall \cos((\alpha+\beta)\pi) + i\sin((\alpha+\beta)\pi) \neq 0 \in \mathbb{C}^{\times}$.

vii. Finite Order: Let $x = \cos(\alpha\pi) + i\sin)\alpha\pi) \in \mathbb{S}$. Then $x^n = \cos(n\alpha\pi) + i\sin(n\alpha\pi)$. We know from trigonometric identities that $\cos(n\alpha\pi) + i\sin(n\alpha\pi)$ when $n\alpha\pi = 2k\pi, k \in \mathbb{Z}$. Since $\alpha \in \mathbb{Q}, \alpha = \frac{u}{v}$ and $u, v \in \mathbb{Z}$. We can always find $n = 2v$, thus $n\alpha = 2u, u \in \mathbb{Z}$ which gives us the identity.

□

10. For each of the following groups, determine ALL subgroups and draw the subgroup lattice: (a) $\mathbb{Z}_{11}$, (b) $\mathbb{Z}_{16}$, (c) $\mathbb{Z}_{30}$. (Hint: Use the previous exercise.)

    Solution:

$$\begin{tikzcd}
\mathbb{Z}_{11} \arrow[d, dash] \\
\langle 0 \rangle
\end{tikzcd}$$

Figure 3: Subgroup Lattice

$$\begin{tikzcd}
\mathbb{Z}_{16} \arrow[d, dash] \\
\langle 2 \rangle \arrow[d, dash] \\
\langle 4 \rangle \arrow[d, dash] \\
\langle 8 \rangle \arrow[d, dash] \\
\langle 0 \rangle
\end{tikzcd}$$

Figure 4: Subgroup Lattice

$$\begin{tikzcd}
 & \mathbb{Z}_{30} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle 5 \rangle \arrow[d, dash] \arrow[dr, dash] & \langle 2 \rangle \arrow[dl, dash] \arrow[dr, dash] & \langle 3 \rangle \arrow[dl, dash] \arrow[d, dash] \\
\langle 10 \rangle \arrow[dr, dash] & \langle 15 \rangle \arrow[d, dash] & \langle 6 \rangle \arrow[dl, dash] \\
 & \langle 0 \rangle &
\end{tikzcd}$$

Figure 5: Subgroup Lattice

11. Let p be a prime integer and $n \geq 2$. Compute the number of elements in the group $GL(n, \mathbb{F}_p)$. Show the group is always non-abelian and contains a non-trivial center.

    Solution:

    $\mathbb{F}_p$ has p elements. There are n columns of an element in $GL(n, \mathbb{F}_p)$. The first column cannot be a zero column. Thus there are $p^n - 1$ choices. The second column needs to be linearly independent of the first, so subtract away the scalar multiples of the first columns we are left with $p^n - p$ choices. For the third column, we must also be linearly independent of the first and second column, so we have only $p^n - p^2$ choices. Thus, similarly

$$\text{For column } k \text{, there are } p^n - p^{k-1} \text{ choices.}$$

Therefore, the entire group $GL(n, \mathbb{F}_p)$ consists of

$$\prod_{k=1}^{n} (p^n - p^{k-1})$$

elements. Now, we can easily find elements A, B in $GL(2, \mathbb{F}_p), p \geq 2$ where $AB \neq BA$. Since $p \geq 2$, we are guaranteed at least 2 distinct elements $a, b \in \mathbb{F}_p$.

$$\begin{pmatrix} a & b \\ b & b \end{pmatrix} \begin{pmatrix} b & b \\ b & a \end{pmatrix} = \begin{pmatrix} ab + b^2 & 2ab \\ 2b^2 & b^2 + ab \end{pmatrix}$$
$$\begin{pmatrix} b & b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ b & b \end{pmatrix} = \begin{pmatrix} ab + b^2 & 2b^2 \\ 2ab & b^2 + ab \end{pmatrix}$$

Clearly they do not commute. We can always construct new matrix A', B' from the A, B which we already have.

$$A' = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_{n-2} \end{array}\right)$$
$$B' = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & I_{n-2} \end{array}\right)$$

and we see that

$$A'B' = \left(\begin{array}{c|c} AB & 0 \\ \hline 0 & I_{n-2} \end{array}\right)$$
$$B'A' = \left(\begin{array}{c|c} BA & 0 \\ \hline 0 & I_{n-2} \end{array}\right)$$

and since $AB \neq BA$, we have $A'B' \neq B'A$ for $A', B' \in GL(n, F_p), n \geq 2$. Thus $GL(n, F_p)$ is always nonabelian for $n \geq 2$. For nontrivial center, consider

$$M = e \cdot a, a \in \mathbb{F}_p$$

We know that e is the identity of $GL(n, \mathbb{F}_p)$, and M is the scalar multiple of e. Let $N \in GL(n, \mathbb{F}_n)$.

$$MN = (e \cdot a)N = (a \cdot e) \cdot N = a \cdot N = N \cdot a = (N \cdot e) \cdot a = N \cdot (e \cdot a) = NM$$

12. Let $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ in $GL(2, \mathbb{F}_5)$. Find A^{-1} and the order of A.

Solution:

$$\begin{aligned}
\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e \\
A^{-1} &= \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \\
A^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
|A| &= 4
\end{aligned}$$

13. p.202:19
    If $a, b \in G$, prove that $|bab^{-1}| = |a|$

    Solution:

    Proof.

$$\begin{aligned}
|bab^{-1}| &= k \\
(bab^{-1})^k &= e \\
b^k a^k b^{-k} &= e \\
b^k a^k b^{-k} b^k &= eb^k \\
b^k a^k e &= b^k \\
b^{-k} b^k a^k &= b^{-k} b^k \\
a^k &= e \\
|a| &= k \\
|bab^{-1}| &= |a|
\end{aligned}$$

□

14. (a) p.211:2.
        i. List all the cyclic subgroups of D_4.

        Solution:

$$\langle e\rangle, \langle r\rangle, \langle r^2\rangle, \langle s\rangle, \langle rs\rangle, \langle r^2 s\rangle, \langle r^3 s\rangle,$$

        ii. List at least one subgroup of D_4 that is not cyclic.

$$H = \{e, r^2, s, r^2 s\}$$

    (b) Find three subgroups of D_4 of order 4.

Solution:

$$\begin{aligned} H_1 &= \langle r \rangle, \\ H_2 &= \{e, r^2, s, r^2 s\} \\ H_3 &= \{e, rs, r^2, r^3 s\} \end{aligned}$$

(c) Draw a picture of the lattice of all subgroups of D_4 you have now found using (a) and (b). There should be ten subgroups in your lattice. (We do not yet know if we have found all subgroups, but it turns out we have.)

Solution:

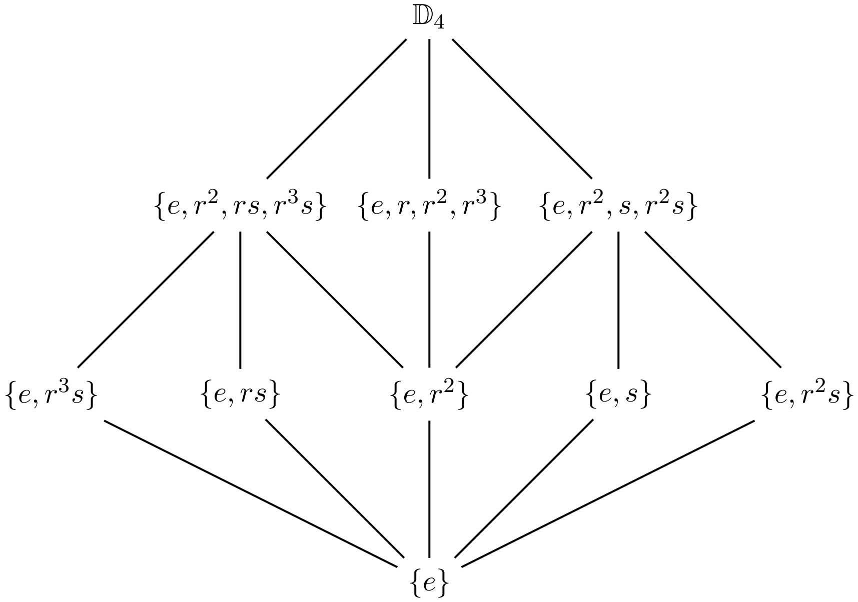

Figure 6: Subgroup Lattice

Problems to look at but DO NOT TURN IN

1. section 7.1: 2,3,8,23,30,33,34
2. section 7.2: 20,32
3. section 7.3: 1,2,4,5,6,7,38,40,45

University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25th May, 2021
Zhewen Zheng

Homework 2

Problems to TURN IN

1. Recall our discussion of the Primitive Root Theorem in lecture 3. Final answers should always be least residues mod n when appropriate.

(a) Verify that 2 is a primitive root in $\mathbb{F}_{13}$.

Solution:

$$\langle 2 \rangle = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\} = \mathbb{F}_{13}$$

(b) Using (a), determine ALL of the primitive roots in $\mathbb{F}_{13}$.

$$|6| = 12, |7| = 12, |11| = 12$$

(c) List ALL of the non-zero squares in $\mathbb{F}_{13}$; i.e. all elements of the form b^2 for some $b \in \mathbb{F}_{13}$. These are the non-zero elements with square roots in $\mathbb{F}_{13}$.

Solution:

$$\begin{aligned} 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12, 6^2 = 10, \\ 7^2 = 10, 8^2 = 12, 9^2 = 3, 10^2 = 9, 11^2 = 4, 12^2 = 12 \\ \{1, 3, 4, 9, 10, 12\} \end{aligned}$$

(d) Create a table that lists the order of each element in $\mathbb{F}_{13}^{\times}$. (This will be easy using (a) and results in lecture 3.)

Solution:

.	
1	1
2	12
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

(e) Verify that $[1+x]$ is a primitive root in the polynomial congruence field of 9 elements $\mathbb{F}_3[x]/(x^2+1)$.

Solution:

$$\begin{aligned}
1+x &= 1+x \\
(1+x)^2 &= x^2+2x+1 = 2x \\
(1+x)^3 &= 2x^2+2x = 1+2x \\
(1+x)^4 &= 2 \\
(1+x)^5 &= 2+2x \\
(1+x)^6 &= x \\
(1+x)^7 &= 2+x \\
(1+x)^8 &= 1
\end{aligned}$$

2. In this exercise, we work out the matrices for the rotational symmetries of the tetrahedron, as studied in HW1. Begin by specifying these four vectors in $\mathbb{R}^3$: $v_1 = (1,1,1)$, $v_2 = (-1,-1,1)$, $v_3 = (1,-1,-1)$, $v_4 = (-1,1,-1)$. Use these as the vertices of your tetrahedron. As in HW1, let r be the rotation around the axis v_1 and s rotation around the axis connecting the midpoints of the line segments $[v_2, v_3]$ and $[v_1, v_4]$.

(a) Write each of the standard basis vectors $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$ in terms of v_1, v_2, v_3, v_4.

Solution:

$$e_1 = \frac{1}{2}(v1+v3), e_2 = \frac{1}{2}(v1+v4), e_3 = \frac{1}{2}(v_1+v_2)$$

(b) Find the matrices for r and s in $O(3,\mathbb{R})$.

Solution:

For s:

$$\begin{aligned}
Be_1 &= \frac{1}{2}(Bv_1 + Av_3) = \frac{1}{2}(v_4 + v_2) = \left(\begin{smallmatrix} -1 \\ 0 \\ 0 \end{smallmatrix}\right) \\
Be_2 &= \frac{1}{2}(Bv_1 + Av_4) = \frac{1}{2}(v_4 + v_1) = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right) \\
Be_3 &= \frac{1}{2}(Bv_1 + Av_2) = \frac{1}{2}(v_4 + v_3) = \left(\begin{smallmatrix} 0 \\ 0 \\ -1 \end{smallmatrix}\right) \\
B &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}
\end{aligned}$$

For r:

$$\begin{aligned}
Ae_1 &= \frac{1}{2}(Av_1 + Av_3) = \frac{1}{2}(v_1 + v_4) = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right) \\
Ae_2 &= \frac{1}{2}(Av_1 + Av_4) = \frac{1}{2}(v_1 + v_2) = \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) \\
Ae_3 &= \frac{1}{2}(Av_1 + Av_2) = \frac{1}{2}(v_1 + v_3) = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right) \\
A &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}
\end{aligned}$$

(c) Use HW1:2 to write down the matrices of all 12 elements of the rotational symmetry group of the tetrahedron. Verify that all 12 elements lie in $SO(3, \mathbb{R})$.

Solution:

$$e^T = e^{-1} \qquad \det e = 1$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{-1} \qquad \det \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 1$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{2T} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{2-1} \qquad \det \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^2 = 1$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^T = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \qquad \det \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1$$

$$\begin{aligned}
(AB)^T &= B^TA^T = B^{-1}A^{-1} = (AB)^{-1} & \det(AB) = 1\\
(A^2B)^T &= B^T(A^2)^T = B^{-1} = (A^2)^{-1} = (A^2B)^{-1} & \det(A^2B) = 1\\
(BA)^T &= A^TB^T = A^{-1}B^{-1} = (BA)^{-1} & \det(BA) = 1\\
(ABA)^T &= A^TB^TA^T = A^{-1}B^{-1}A^{-1} = (ABA)^{-1} & \det(ABA) = 1\\
(A^2BA)^T &= A^TB^T(A^2)^T = A^{-1}B^{-1}(A^2)^{-1} = (A^2BA)^{-1} & \det(A^2BA) = 1\\
(BA^2)^T &= (A^2)^TB^T = (A^2)^{-1}B^{-1} = (BA^2)^{-1} & \det(BA^2) = 1\\
(ABA^2)^T &= (A^2)^TB^TA^T = (A^2)^{-1}B^{-1}A^{-1} = (ABA^2)^{-1} & \det(ABA^2) = 1\\
(A^2BA^2)^T &= (A^2)^TB^T(A^2)^T = (A^2)^{-1}B^{-1}(A^2)^{-1} = (A^2BA^2)^{-1} & \det(A^2BA^2) = 1
\end{aligned}$$

3. Let G^r be the rotational symmetry group of the tetrahedron.

   (a) Construct an injective map $\Theta : G^r \mapsto S_4$.

$$\begin{aligned}
e &\mapsto (1)(2)(3)(4)\\
r &\mapsto (243)\\
r^2 &\mapsto (234)\\
s &\mapsto (14)(23)\\
rs &\mapsto (142)\\
r^2s &\mapsto (143)\\
sr &\mapsto (134)\\
rsr &\mapsto (132)\\
r^2sr &\mapsto (13)(24)\\
sr^2 &\mapsto (124)\\
rsr^2 &\mapsto (12)(34)\\
r^2sr^2 &\mapsto (123)
\end{aligned}$$

   (b) Describe the image of Θ; i.e. which permutations in S_4 correspond to rotational symmetries of the tetrahedron?

   Solution:

   The kind of permutation with partition $[3,1], [2,2], [1,1,1,1]$ in S_4 correspond to rotational symmetries of the tetrahedron.

   (c) Give an example of a permutation in S_4 that does NOT correspond to a rotational symmetry of the tetrahedron. Does it represent a symmetry?

   Solution:

   (1234) does not correspond to a rotational symmetry of the tetrahedron. However, if we include the reflectional symmetries, we can achieve (1234) by applying rs and then do a reflection across the plane defined by $1, 4$ and the mid point of 2 and 3.

4. Let $\omega_n = e^{\frac{2\pi i}{n}}$ for $n \geq 2$. Form the matrix

$$r_n = \begin{pmatrix} \omega_n & 1 \\ 0 & 1 \end{pmatrix}$$

Prove that r_n is an element of finite order in $GL(2, \mathbb{C})$. What is the order?

Solution:

Proof. Let $\omega_n = e^{\frac{2\pi i}{n}}, n \geq 2$.

$$r_n = \begin{pmatrix} \omega_n & 1 \\ 0 & 1 \end{pmatrix}$$
$$r_n^2 = \begin{pmatrix} \omega_n^2 & \omega_n \\ 0 & 1 \end{pmatrix}$$

Induction Hypothesis:

$$r_n^k = \begin{pmatrix} \omega_n^k & \sum_{i=0}^{k-1} \omega_n^i \\ 0 & 1 \end{pmatrix}$$

Inductive Case:

$$\begin{aligned} r_n^{k+1} &= \begin{pmatrix} \omega_n^k & \sum_{i=0}^{k-1} \omega_n^i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_n & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \omega_n^{k+1} & \omega_n^k + \sum_{i=0}^{k-1} \omega_n^i \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \omega_n^{k+1} & \sum_{i=0}^{k} \omega_n^i \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Thus

$$\det(r_n^k) = (\omega_n^k) = e^{\frac{2\pi i}{n}} \neq 0$$

since $e^s \neq 0$ for all $s \in \mathbb{C}$. Thus $r_n \in GL(2, \mathbb{C})$.
Now, by the geometric sequence formula, $\sum_{i=0}^{k} \omega_n^i = \frac{1-\omega_n^k}{1-\omega_n}$. Thus, observe that if $n \mid k$ then $mn = k$ for some $m \in \mathbb{Z}+$.

$$\begin{aligned} \frac{1-\omega_n^k}{1-\omega_n} &= \frac{1 - e^{\left(\frac{2\pi i}{n}\right)^k}}{1-\omega_n} \\ &= \frac{1-(-1)^2 m}{1-\omega_n} \\ &= 0 \end{aligned}$$

where $\omega_n^k = (-1)^{2m} = 1$. Thus we obtain

$$r_n^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The order of r_n thus is the least positive power k, thus m must be minimized, and therefore $|r_n| = k = n$

□

5. p.202: 26

   Prove that every nonabelian group G has order at least 6; hence, every group of order 2,3,4, or 5 is abelian. [Hint: If $a, b \in G$ and $ab \neq ba$, show that the elements of the subset $H = \{e, a, b, ab, ba\}$ are all distinct. Show that either $a^2 \notin H$ or $a^2 = e$, in the latter case, verify that $aba \notin H$.]

   Solution:

   Proof. For order 2 Let $a, b \in G, ab \neq ba$. Now, if $a = b$ then $ab = a^2 = ba$. Contradiction. Thus $a \neq b$. If $a = e$ or $b = e$ then $ab = eb = ea = ba$, contradiction. Thus elements of the subset $H = \{e, a, b, ab, ba\}$ are all distinct. Consider a^2.

$$a^2 \neq a \neq b \neq ab \neq ba$$

   otherwise would contradict $ab \neq ba$. Thus either $a^2 = e$ or $a^2 \notin H$. In the first case, consider aba

$$\begin{aligned}
aba &= e \\
aba &= a^2 \\
ab &= a = ba \quad \text{contradiction} \\
aba &= a \\
aba &= a^3 \\
ab &= a^2 = ba \quad \text{contradiction} \\
aba &= b \\
aba &= ba^2 \\
ab &= ba \quad \text{contradiction} \\
aba &= ab \\
ba &= b \\
a &= e \quad \text{contradiction} \\
aba &= ba \\
ab &= b \\
a &= e \quad \text{contradiction}
\end{aligned}$$

   Hence $aba \notin H$. In both case H is not closed. Thus every group of order 2,3,4,5 is abelian. □

6. p.213: 54

   If $G \neq \langle e \rangle$ is a group that has no proper subgroups, prove that G is a cyclic group of prime order.

   Solution:

   Proof. Let $G \neq \langle e \rangle$ be a group with no proper subgroups. Thus the only subgroups to G are G and $\langle e \rangle$. Consider an element $a \in G$. By Theorem 7.14 $\langle a \rangle$ is a subgroup of G. $\langle a \rangle \neq \langle e \rangle$, so it must be $\langle a \rangle = G$. Thus G is cyclic. If $|G| = \infty$, then $G \cong \mathbb{Z}$, but $\mathbb{Z}$ has nontrivial proper subgroups. So $|G| < \infty$. Suppose $|G| = n$. Then $G \cong \mathbb{Z}_n$. Now, since G is cyclic, we know that for every $d \mid k$ there exists a subgroup H with $|H| = d$ (Follows directly from Theorem 7.9 (3); If $n = td, d \geq 1$ then $|a^t| = |\langle a^t \rangle| = d$, $\langle a^t \rangle$ is a subgroup of H. Also, we can see the same thing from $\mathbb{Z}_n$). Thus we need the only divisors of n to be 1 and d. Therefore $n = |G|$ must be prime. □

7. p.235: 21

Find the order of σ^{1000}, where σ is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$. [Hint: Write σ as a product of disjoint cycles.]

Solution:

$$\begin{aligned} \sigma &= (138)(27)(4965) = (4965)(138)(27) \\ |\sigma| &= \operatorname{lcm}(4,3,2) = 12 \\ \sigma^{1000} &= \sigma^{1000 \mod 12} = \sigma^4 \end{aligned}$$

By Theorem 7.9,

$$\begin{gathered} 12 = 4 \cdot 3 \\ |\sigma^{1000}| = |\sigma^4| = 3 \end{gathered}$$

8. p.235: 22

Show that S_{10} contains elements of orders 10,20, and 30. Does it contain an element of order 40?

Solution:

$$\begin{aligned} \tau &= (12345)(67)(89)(10) \\ |\tau| &= \operatorname{lcm}(5,2,1) = 10 \\ \sigma &= (12345)(6789)(10) \\ |\sigma| &= \operatorname{lcm}(5,4,1) = 20 \\ \rho &= (12345)(678)(9\,10) \\ |\rho| &= \operatorname{lcm}(5,3,2) = 30 \end{aligned}$$

Consider divisor of 40 that are less or equal to 10. They are $1, 2, 4, 5, 8, 10$. Now, for partition containing 1, the maximum lcm is given by $\operatorname{lcm}(5,4,1) = 20$. For partition containing 2, the maximum lcm is given by $\operatorname{lcm}(5,3,2) = 30$. For partition containing 4, the maximum lcm is given by $\operatorname{lcm}(5,4,1) = 20$. For partition containing 5, the maximum lcm is given by $\operatorname{lcm}(5,3,2) = 30$. For partition containing 8, the maximum lcm is given by $\operatorname{lcm}(8,1,1) = \operatorname{lcm}(8,2,1) = 8$. For partition containing 10, the maximum lcm is given by $\operatorname{lcm}(10) = 10$. There is no partitioning of S_{10} capable of giving out a lcm of 40. Therefore, it does not contain an element of order 40.

9. p.235: 30
   Prove that every element of A_n is a product of 3-cycles.

   Solution:

   Proof. Every element of A_n is an even permutation. We just need to show that all even permutations can be expressed as a product of 3-cycles. Let $m \in A_n, m = (ij)(kl)$. There are two cases: (ij) and (kl) are either joint or disjoint. In case that (ij) and (kl) are joint, then WLOG let $j = k$, we have

   $$(ij)(kl) = (ij)(jl) = (ijl)$$

   for any $i, j = k, l$. For the case that (ij) and (kl) are disjoint, we have

   $$(ij)(kl) = (ijk)(jkl)$$

   As we can see in the figure They are the same. Now, every even permutation are composed of even number of transpositions, which we have proved that any even pair of transposition can be expressed as a product of 3-cycles. Thus every element of A_n is a product of 3-cycles. □

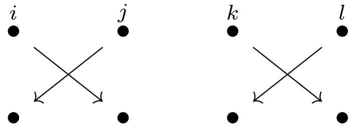

Figure 7: Mapping 1

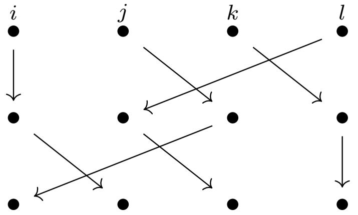

Figure 8: Mapping 2

10. p.235: 36
    If τ is the k-cycle $(a_1 a_2 \cdots a_k)$ and if $\sigma \in S_n$, prove that $\sigma\tau\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$.

    Solution:

    Proof. We need to prove that

    (a) $\sigma\tau\sigma^{-1}(a_i) = \begin{cases} \sigma(a_{i+1}) & 1 \le i < k \\ \sigma(a_1) & i = k \end{cases}$

(b) $\sigma\tau\sigma^{-1}$ fixes elements not in the cycle $(\sigma(a_1)\cdots\sigma(a_k))$; If $\sigma(a_i) \neq m$ for $1 \leq i \leq k$, we have $\sigma\tau\sigma^{-1}(m) = m$.

First consider any a_i where $1 \leq i \leq k$. Then

$$\tau(a_i) = \begin{cases} a_{i+1} & 1 \leq i < k \\ a_1 & i = k \end{cases}$$

Now, notice

$$\begin{aligned} \sigma\tau\sigma^{-1}(\sigma(a_i)) &= \sigma\tau(\sigma^{-1}\sigma)(a_i) \\ &= \sigma\tau(a_i) \\ &= \begin{cases} \sigma(a_{i+1}) & 1 \leq i < k \\ \sigma(a_1) & i = k \end{cases} \end{aligned}$$

which agrees with the RHS of the equation. Now, consider any element $m \neq \sigma(a_i)$ for $1 \leq i \leq k$. Then we know that

$$\begin{aligned} \sigma^{-1}(m) &\neq \sigma^{-1}\sigma(a_i) \\ \sigma^{-1}(m) &\neq a_i \end{aligned}$$

for $1 \leq i \leq k$. By definition of τ, then

$$\begin{aligned} \tau\sigma^{-1}(m) &= \sigma^{-1}(m) \\ \sigma\tau\sigma^{-1}(m) &= \sigma\sigma^{-1}(m) \\ \sigma\tau\sigma^{-1}(m) &= m \end{aligned}$$

Indeed, when $\sigma(a_i) \neq m$ for $1 \leq i \leq k$, we have $\sigma\tau\sigma^{-1}(m) = m$. □

11. For $n = 3, 4$, construct a table: for each partition of n list all elements of S_n having a disjoint cycle decomposition of that partition type, then the order of each element of a given partition type. Finally, in your table, circle the elements of S_n that are in A_n.

Solution:

$n = 3$	elements	order
$[3]$	[✓ $(123), (132)$]	3
$[2, 1]$	$(12), (13), (23)$	2
$[1, 1, 1]$	[✓ e]	1

$n = 4$	elements	order
$[4]$	$(1234), (1243), (1324), (1342), (1423), (1432)$	4
$[3, 1]$	[✓ $(123), (124), (132), (134), (142), (143), (234), (243)$]	3
$[2, 2]$	[✓ $(12)(34), (13)(24), (14)(23)$]	2
$[2, 1, 1]$	$(12), (13), (14), (23), (24), (34)$	2
$[1, 1, 1, 1]$	[✓ e]	1

12. Find all numbers k so that S_8 has an element of order k. (Note: This question and the analog for S_{12} arises when trying to mathematically understand all moves of the Rubik's cube and find the move of largest order. It turns out that 1260 is the largest order of an element of the Rubic Cube group.)

    Solution:

$n = 8$	order
$[8]$	8
$[7, 1]$	7
$[6, 2]$	6
$[6, 1, 1]$	6
$[5, 3]$	15
$[5, 2, 1]$	10
$[5, 1, 1, 1]$	5
$[4, 4]$	4
$[4, 3, 1]$	12
$[4, 2, 2]$	4
$[4, 2, 1, 1]$	4
$[4, 1, 1, 1, 1]$	4
$[3, 3, 2]$	6
$[3, 3, 1, 1]$	3
$[3, 2, 2, 1]$	6
$[3, 2, 1, 1, 1]$	6
$[3, 1, 1, 1, 1, 1]$	3
$[2, 2, 2, 2]$	2
$[2, 2, 2, 1, 1]$	2
$[2, 2, 1, 1, 1, 1]$	2
$[2, 1, 1, 1, 1, 1, 1]$	2
$[1, 1, 1, 1, 1, 1, 1, 1]$	1

13. In this problem we will work in S_4.

    (a) Find all subgroups of order 2 or 3.

    Solution:

    Order 2:

$$\{e, (12)\}, \{e, (13)\}, \{e, (14)\}, \{e, (23)\}, \{e, (24)\}, \{e, (34)\},$$
$$\{e, (12)(34)\}, \{e, (13)(24)\}, \{e, (14)(23)\}$$

    Order 3:

$$\{e, (123), (132)\}, \{e, (124), (142)\}, \{e, (134), (143)\}, \{e, (234), (243)\}$$

    (b) Find three different subgroups each of which is isomorphic to D_4.

Solution:

$$\langle (1234), (24) \rangle, \langle (1324), (34) \rangle, \langle (1432), (42) \rangle$$

(c) Find four different subgroups of order 6. Are any of these cyclic?

Solution:

$$\langle (123), (13) \rangle, \langle (124), (14) \rangle, \langle (134), (14) \rangle, \langle (234), (24) \rangle$$

No. Suppose there exists a cyclic subgroup of order 6. That would imply that there exists an element $a \in S_4$ such that $|a| = 6$, which is impossible (see table in #11).

Problems to look at but DO NOT TURN IN

1. section 7.3: 53, 56
2. section 7.4: 3,4,10,32
3. section 7.5: 1,2,3,4,5,6,8,11,18,19,20

University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25th May, 2021
Zhewen Zheng

Homework 3

Problems to TURN IN

1. Section 8.1: 6
   $K = \langle 3\rangle; G = \mathbb{U}_{32}$. G is a group and K is a subgroup of G. List the distinct right cosets of K in G.

   Solution:

   $$\begin{aligned} K &= \langle 3\rangle = \{1, 3, 9, 11, 17, 19, 25, 27\} \\ G &= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\} \end{aligned}$$

   We want to find all distinct Ka where $a \in G$. Now, since K is cyclic, we know that

   $$K = Ke = K3 = K9 = K11 = K17 = K19 = K25 = K27$$

   Now consider K5

   $$K5 = \{5, 15, 13, 23, 21, 31, 29, 7\}$$

   Since $7, 13, 15, 21, 23, 29, 31 \in K5$, notice

   $$\begin{aligned} 7 &= 3^j 5 \\ 7 &= k5, k \in K \\ 7 \cdot 5^{-1} &= k, k \in K \\ 7 \cdot 5^{-1} &\in K \\ 7 &\equiv 5 \pmod{K} \end{aligned}$$

   By Theorem 8.2 $K7 = K5$. The same argument suffices for all the other $a \in K5$.

   $$K5 = K7 = K13 = K15 = K21 = K23 = K29 = K31$$

   Thus far, all possible right cosets have been considered and therefore the distinct right cosets of K in G are:

   $$G = \{K \cup K5\}$$

2. Section 8.1: 12

   (a) Let $K = \{(1), (12)(34), (13)(24), (14)(23)\}$. Show that K is a subgroup of A_4 and hence, a subgroup of S_4.[Hint. Theorem 7.12].

Solution:

See below that K is closed under the operation in G. By Theorem 7.12 K is a subgroup of A_4 thus a subgroup of S_4.

$$\begin{aligned}(12)(34)\cdot(13)(24) &= (14)(23)\\ (13)(24)\cdot(12)(34) &= (14)(23)\\ (12)(34)\cdot(14)(23) &= (13)(24)\\ (14)(23)\cdot(12)(34) &= (13)(24)\\ (13)(24)\cdot(14)(23) &= (12)(34)\\ (14)(23)\cdot(13)(24) &= (12)(34)\end{aligned}$$

(b) State the number of cosets of K in A_4. Don't list them.

Solution:

$$[A_4 : K] = \frac{|A_4|}{|K|} = \frac{12}{4} = 3$$

(c) State the number of cosets of K in S_4. Don't list them.

Solution:

$$[S_4 : K] = \frac{|S_4|}{|K|} = \frac{24}{4} = 6$$

3. Section 8.1: 14
   $G = S_4; K$ is the subgroup of Exercise 12. K is a subgroup of G. Determine whether the given cosets are disjoint or identical.

   (a) $K(12)$ and $K(34)$

   Solution:

   $K(12) = K(34)$ if and only if $(12)((34)^{-1}) \in K$.

   $$\begin{aligned}(34)^{-1} &= (34)\\ (12)((34)^{-1}) &= (12)(34) \in K\end{aligned}$$

   Thus $K(12) = K(34)$.

   (b) $K(1234)$ and $K(1324)$ $K(1234) = K(1324)$ if and only if $(1234)((1324)^{-1}) \in K$.

   $$\begin{aligned}(1324)^{-1} &= (1423)\\ (1234)((1324)^{-1}) &= (1234)(1423) = (243) \notin K\end{aligned}$$

   Thus $K(1234)$ and $K(1324)$ are not identical, thus disjoint.

4. Section 8.1: 18
   Give examples, other than those in the text, of infinite groups G and H such that

   (a) $[G : H]$ is finite

Solution:

$$G = \mathbb{Z}, H = \mathbb{Z}, [G : H] = 1$$

(b) $[G : H]$ is infinite

$$G = \mathbb{Q}, H = \mathbb{Z}, [G : H] = \infty$$

5. Section 8.1: 22
If H and K are subgroups of a finite group G, prove that $|H \cap K|$ is a common divisor of $|H|$ and $|K|$.

Solution:

Proof. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since H is a subgroup, $a \cdot b \in H$; since K is a subgroup, $a \cdot b \in K$. Thus $a \cdot b \in H \cap K$. Next, check closure under inverses. Let $a \in H \cap K$. Then $a \in H$ and $a \in K$. Since H and K are subgroups, $a^{-1} \in H$ and $a^{-1} \in K$. Thus $a^{-1} \in H \cap K$. We also know that $H \cap K$ is not empty since $e \in H$ and $e \in K$ which gives us $e \in H \cap K$. Therefore $H \cap K$ is a subgroup of H and K and G. Thus by Lagrange's Theorem,

$$|H \cap K| \mid |H|, |H \cap K| \mid |K|$$

thus $|H \cap K|$ is a common divisor of $|H|$. □

6. Section 8.1: 26
Prove that a group of order 8 must contain an element of order 2.

Solution:

Proof. Let G be a group of order 8. Then $|G| = 8$. Let K be a subgroup of G, by Lagrange's Theorem, $a \in G$ can only have $|a| = 1, 2, 4, 8$. If $|a| = 8$, then $|a^3| = 2$. If $|a| = 4$ then $|a^2| = 2$. Suppose then all nontrivial elements of G has order 3. Then for any element a we must have $a \neq a^{-1}$, which means that we can always find pairs of a with its inverse. Since inverses are unique, that means we also had unique elements pairs, giving us an even number of elements without counting the identity. This implies that $|G|$ is odd, which is a contradiction. Thus a group of order 8 must contain an element of order 2. □

7. Section 8.1: 30
Let H and K be subgroups of an infinite group G such that $K \subseteq H$, $[G : H]$ is finite, and $[H : K]$ is finite. Prove that $[G : K]$ is finite and $[G : K] = [G : H][H : K]$. [Hint: Let $Ha_1, Ha_2, \cdots, Ha_n$ be the disinct cosets of H in G and let $Kb_1, Kb_2, \cdots, Kb_m$ be the distinct cosets of K in H. Show that Kb_ia_j (with $1 \leq i \leq m$ and $1 \leq j \leq n$) are the distinct cosets of K in G.]

Solution:

Proof. Let $Ha_1, Ha_2, \cdots, Ha_n$ be the disinct cosets of H in G and let $Kb_1, Kb_2, \cdots, Kb_m$ be the distinct cosets of K in H. To show that we can map the distinct cosets of G, namely Ha_j for some j, to Kb_ia_j, we consider the following map: $\phi(Kb_ia_j) = (Ha_i, Kb_j)$.

$$\begin{aligned} b_i \in H, Kb_{i_1}a_{j_1} = Kb_{i_2}a_{j_2} &\implies b_{i_1}a_{j_1} \equiv b_{i_2}a_{j_2} \pmod{K} \\ Kb_{i_1}a_{j_1} \subset Ha_{j_1}, Kb_{i_2}a_{j_2} \subset Ha_{j_2} & \\ a_{j_1} = a_{j_2} & \\ Kb_{i_1}a_j = Kb_{i_2}a_j & \\ Kb_{i_1}a_j(a_j)^{-1} = Kb_{i_2}a_j(a_j)^{-1} & \\ Kb_{i_1} = Kb_{i_2} & \\ b_{i_1} = b_{i_2} & \end{aligned}$$

Now the map is injective. To see it's surjective, observe that for all cosets $Kb_i \subseteq Ha_j$ for all cosets $Ha_j \subseteq G$, there exists a Kb_ia_j such that $\phi(Kb_ia_j) = (Ha_i, Kb_j)$. Thus the maps is surjective.

□

8. Section 8.1: 44

   (a) Show that A_4 (which has order 12 by Theorem 7.29) has exactly three elements of order 2.

   Solution:

   The only nontrivial elements in A_4 are 3-cycles (such as $(123), (124)$) which all have order 3, and the disjoint transpositions, which are $(12)(34), (13)(24), (14)(23)$. Only these three elements are order 2.

   (b) Prove that the elements of order 2 and the identity element form a subgroup.

   Solution:

   Proof.

   $$K = \{(1), (12)(34), (13)(24), (14)(23)\}$$

   See proof in problem 2 that K is a subgroup of A_4. □

   (c) Prove that A_4 has no subgroup of order 6. Hence, the converse of Lagrange's Theorem is false. [Hint: If N is a subgroup of order 6, use Theorem 8.9 to determine the structure of N and use part (b) to reach a contradiction.]

Solution:

Proof. Suppose we have H, a subgroup of A_4 with order 6. By Theorem 8.9, H is either isomorphic to $\mathbb{Z}_6$ or S_3. Because A_4 has no element with order 6, H cannot be isomorphic to $\mathbb{Z}_6$. Then $H \cong S_3$. We know that S_3 has three element of order 2. By part (b), we know that A_4 also has exactly three element of order 2. However, we also know that the elements of order 2 and the identity element from a subgroup K of order 4. By Lagrange, $H \cong S_3$ and $|H| = 6$, and we should have $|K| \mid |H| = 4 \mid 6$. Contradiction. Thus A_4 must not have a subgroup H with order 6. □

9. Let G and H be the following subgroups of $GL(2, \mathbb{R})$:

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x > 0 \right\} \quad H = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x > 0 \right\}$$

An element of G can be represented by a point in the open right half plane $\mathcal{P}$. Draw a picture of the partitioning of $\mathcal{P}$ into left and right cosets of H.

Solution:

Consider

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$$

as a point $(x, y) \in \mathbb{R}^2$. Then G is the open right half plane $\mathcal{P}$. The left coset:

$$\begin{aligned} gH &= \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a > 0 \right\} \\ &= \left\{ \begin{pmatrix} ax & y \\ 0 & 1 \end{pmatrix} : a > 0 \right\} \end{aligned}$$

The right coset:

$$\begin{aligned} Hg &= \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : a > 0 \right\} \\ &= \left\{ \begin{pmatrix} ax & ay \\ 0 & 1 \end{pmatrix} : a > 0 \right\} \end{aligned}$$

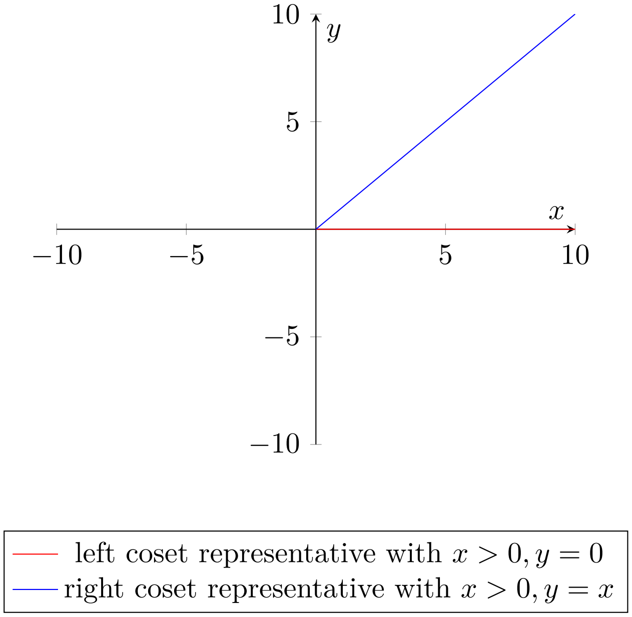

Figure 9: Picture for specific representative in left and right cosets

The left cosets, are the horizontal rays with y given by the choice of $g \in G$. The right cosets, are the rays starting from origin pointing toward the positive x direction with any slope a given by H.

10. Section 8.2: 10
If G is a group, prove that every subgroup of $Z(G)$ is normal in G. [Compare with Exercise 14.]

Solution:

Proof. Let $a \in G, z \in Z(G)$.

$$\begin{aligned} az &= za \\ az &\in Z(G)a \\ aZ(G) &\subseteq Z(G)a \\ aZ(G)a^{-1} &\subseteq Z(G) \end{aligned}$$

By Normality Theorem 8.11, $Z(G)$ is a normal subgroup of G. □

11. Section 8.2: 14
Show by example that if M is a normal subgroup of N and if N is a normal subgroup of a group G, then M need not be a normal subgroup of G; in other words, normality isn't transitive. [Hint: Consider $M = \{v, r_0\}$ and $N = \{h, v, r_2, r_0\}$ in D_4.]

Solution:

Proof. Consider $N = \{r_0, r_2, h, v\} \subseteq G$. N is normal since $N \cong V$ where $V = \{e, (12)(34), (13)(24), (14)(23)\}$. (Label D_4 with $1, 2, 3, 4$ starting from negative x direction in a counter clockwise order.) V is normal. Let $\tau = (ab)(cd) \in V, \sigma \in G$

$$\begin{aligned}\sigma\tau\sigma^{-1} &= \sigma(ab)(cd)\sigma^{-1}\\ &= \sigma(ab)\sigma^{-1}\sigma(cd)\sigma^{-1}\\ &= (\sigma(a)\sigma(b))(\sigma(c)\sigma(d)) \in V\end{aligned}$$

Since V is normal, N is normal in G. However, M is not a normal subgroup of G; for example

$$\begin{aligned}M &= \{e, (14)(23)\}\\ (24)(14)(23)(24)^{-1} &= (24)(14)(23)(24)\\ &= (12)(34) \notin M\end{aligned}$$

□

12. Section 8.2: 24
Let $N = \{A \in GL(2, \mathbb{R}) \mid \det A \in \mathbb{Q}\}$. Prove that N is a normal subgroup of $GL(2, \mathbb{R})$. [Hint: Exercise 32 of Section 7.4.]

Solution:

Proof. Let $A \in N$, $B \in G = GL(2, \mathbb{R})$. Now,

$$\begin{aligned}BAB^{-1} &= C \in GL(2, \mathbb{R}),\\ \det(BAB^{-1}) &= \det(B)\det(A)\det(B^{-1})\\ &= \det(A) \in \mathbb{Q}\end{aligned}$$

By the normality theorem N is a normal subgroup of $GL(2, \mathbb{R})$. □

13. Section 8.2: 29
Let N be a cyclic normal subgroup of a group G, and H any subgroup of N. Prove that H is a normal subgroup of G. [Compare Exercise 14.]

Solution:

Proof. Let N be a cyclic normal subgroup of a group G, and H any subgroup of N. By Theorem 7.17, H is cyclic and $H = \langle n^d \rangle$ for some $d \geq 1$.

$$\begin{aligned}N &= \langle n \rangle\\ gNg^{-1} &= N\\ g(n^i)g^{-1} &= n^j\end{aligned}$$

now, for any $d \geq 1$,

$$\begin{aligned} g(n^d)^i g^{-1} &= g(n^i)^d g^{-1} \\ &= \underbrace{(g(n^i)g^{-1})(g(n^i)g^{-1})\cdots(g(n^i)g^{-1})}_{d} \\ &= (g(n^i)g^{-1})^d \\ &= (n^j)^d \\ &= (n^d)^j \in H \end{aligned}$$

By the Normality theorem H is a normal subgroup of G. □

14. Return to lecture 9 where we determine the lattice of all subgroups of D_4. Determine ALL normal subgroups of D_4.

    Solution:

    By definition of D_4, we have $dr = r^{-1}d$. To find normal subgroups of D_4, we can first find the subgroups with index 2. Reading from the lattice we have

    $$\{e, d, r^2d, r^2\}, \{e, r, r^2, r^3\}, \{e, r^2, rd, r^3d\}$$

    These are given by the Lemma which states subgroups with index 2 are normal. Now, the only possible normal subgroups can be only picked from the subgroups with order 2. We know that $\{e, r^2\}$ is subgroup of $Z(D_4)$ and thus is normal. All other subgroups can be easily found to be not normal by example

    $$\begin{aligned} r\{e, d\}r^{-1} &\neq \{e, d\} \\ r\{e, r^2d\}r^{-1} &\neq \{e, r^2d\} \\ r\{e, rd\}r^{-1} &\neq \{e, rd\} \\ r\{e, r^3d\}r^{-1} &\neq \{e, r^3d\} \end{aligned}$$

15. Section 8.3: 2
    Let G be the subgroup $\langle 3 \rangle$ of $\mathbb{Z}$, and let N be the subgroup $\langle 15 \rangle$. Find the order of $6 + N$ in the group G/N.

    Solution:

    G/N consists 15 cosets: $N + 0, N + 1, \cdots, N + 14$.

    $$\begin{aligned} G &= \{\cdots, -3, 0, 3, 6\cdots\} \\ N &= \{\cdots, -15, 0, 15, 30\cdots\} \\ (N + 6)^5 &= (N + 12)(N + 6)^3 = (N + 18)(N + 6)^2 = (N + 24)(N + 6) = N + 0 \end{aligned}$$

16. Section 8.3: 6
    Show that $\mathbb{Z}_6/N \cong \mathbb{Z}_3$, where N is the subgroup $\{0, 3\}$.

Solution:

$$\begin{aligned} N+0 &= \{0,3\} \\ N+1 &= \{1,4\} \\ N+2 &= \{2,5\} \\ \mathbb{Z}_6/N &= (N+0)\cup(N+1)\cup(N+2) \\ |\mathbb{Z}_6/N| &= 3 \end{aligned}$$

By the Classification Theorem (or Theorem 8.7)

$$\mathbb{Z}_6/N \cong \mathbb{Z}_3$$

17. Section 8.3: 10

(a) Let M be the cyclic subgroup $\langle(0,2)\rangle$ of the additive group $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ and let N be the cyclic subgroup $\langle(1,2)\rangle$, as in Example 4. Verify that M is isomorphic N.

Solution:

$$\begin{aligned} M &= \{(0,0),(0,2)\}, |M| = |N| \\ \phi &: (0,0) \mapsto (0,0), (0,2) \mapsto (1,2) \end{aligned}$$

ϕ is bijective homomorphism. Thus M is isomorphic N.

(b) Write out the operation table of G/M, using the four cosets $M+(0,0), M+(1,0), M+(0,1), M+(1,1)$.

Solution:

	$M+(0,0)$	$M+(1,0)$	$M+(0,1)$	$M+(1,1)$
$M+(0,0)$	$M+(0,0)$	$M+(1,0)$	$M+(0,1)$	$M+(1,1)$
$M+(1,0)$	$M+(1,0)$	$M+(0,0)$	$M+(1,1)$	$M+(0,1)$
$M+(0,1)$	$M+(0,1)$	$M+(1,1)$	$M+(0,0)$	$M+(1,0)$
$M+(1,1)$	$M+(1,1)$	$M+(0,1)$	$M+(1,0)$	$M+(0,0)$

(c) Show that G/M is not isomorphic to G/N (the operation table for G/N is in Example 4). Thus for normal subgroups M and N, the fact that $M \cong N$ does not imply that G/M is isomorphic to G/N.

Solution:

Notice that there is no single coset that generates G/M, thus G/M not cyclic. However, $|G/M| = 4$, Thus $G/M \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4 \cong G/N$.

18. Section 8.3: 18
Show that $\mathbb{U}_{32}/N \cong \mathbb{U}_16$, where N is the subgroup $\{1,17\}$.

Solution:

$$\mathbb{U}_{32} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}, |\mathbb{U}_{32}| = 16$$

Claim: $\mathbb{U}_{32}/N \cong \mathbb{U}_{16}$.

Proof. Let $\phi : \mathbb{U}_{32}/N \mapsto \mathbb{U}_{16}, \phi(N[a]_{32}) = [a]_{16}$.

(a) Well-defined: Suppose $N[a]_{32} = N[b]_{32}$

$$\begin{aligned}
&\implies [a]_{32} \in N[b]_{32} = \{[b]_{32}, 17b_{32}\} \\
&\implies [a]_{32} = [b]_{32} \text{ or } [a]_{32} = 17[b]_{32} \\
&\implies 32 \mid a - b \text{ or } 32 \mid a - 17b \\
&\implies 16 \mid a - b \text{ or } 16 \mid a - 17b \\
&\implies a \equiv b \pmod{16} \text{ or } a \equiv 17b \pmod{16} \\
&\implies a \equiv b \pmod{16} \text{ or } a \equiv b \pmod{16}
\end{aligned}$$

(b) homomorphism:

$$\begin{aligned}
\phi(N[a]_{32}N[b]_{32}) &= \phi(N[ab]_{32}) \\
&= [ab]_{16} \\
&= [a]_{16}[b]_{16} \\
&= \phi(N[a]_{32})\phi(N[b]_{32})
\end{aligned}$$

(c) Surjective: for all $b \in \mathbb{U}_{16}$, there exists $b \in \mathbb{U}_{32}$ such that

$$\phi(N[b]_{32}) = [b]_{16}$$

Since $|\mathbb{U}_{32}/N| = |\mathbb{U}_{16}| = 8$ and is surjective, thus ϕ is also injective. Therefore $\mathbb{U}_{32}/N \cong \mathbb{U}_{16}$.

□

19. Section 8.3: 24
If G is a cyclic group, prove that G/N is cyclic, where N is any subgroup of G.

Solution:

Proof. Let $G = \langle a \rangle, b \in G$. Then

$$\begin{aligned}
G/N &= \{Nb \mid b \in G\} \\
&= \{Na^i \mid i \in \mathbb{Z}\} \\
&= \{(Na)^i \mid i \in \mathbb{Z}\} \\
&= \langle Na \rangle
\end{aligned}$$

Thus G/N is cyclic. □

20. Section 8.3: 25

(a) Find the order of $\frac{8}{9}, \frac{14}{5}$, and $\frac{48}{28}$ in the additive group $\mathbb{Q}/\mathbb{Z}$.

Solution:

$$9\left(\frac{8}{9}+\mathbb{Z}\right)=\mathbb{Z}$$
$$5\left(\frac{14}{5}+\mathbb{Z}\right)=\mathbb{Z}$$
$$7\left(\frac{48}{28}+\mathbb{Z}\right)=\mathbb{Z}$$

(b) Prove that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

Solution:

Proof. For any element $s \in \mathbb{Q}/\mathbb{Z}$, there is a $r \in \mathbb{Q}$ such that $s = r + \mathbb{Z}$. Then since $r \in \mathbb{Q}, r = \frac{a}{b}$ where $a, b \neq 0 \in \mathbb{Z}$. WLOG let $b > 0$. Then we have $s = \frac{a}{b} + \mathbb{Z}$. Thus

$$bs = b\left(\frac{a}{b}+\mathbb{Z}\right) = a + \mathbb{Z} = \mathbb{Z}$$

And b is finite. Thus any $s \in \mathbb{Q}/\mathbb{Z}$ has finite order. □

(c) Prove that $\mathbb{Q}/\mathbb{Z}$ contains elements of every possible finite order.

Solution:

Proof. For any finite number $n \in \mathbb{N}$, we may have

$$s = r + \mathbb{Z}, r = \frac{1}{n}$$

Now, the order of s is the smallest positive integer t with $n \mid t$. Thus $|s| = t = n$. Since n is arbitrary, for any finite order n we may find such an element in $\mathbb{Q}/Z$. □

21. Section 8.3: 26
Prove that the set of elements of finite order in the group $\mathbb{R}/\mathbb{Z}$ is the subgroup $\mathbb{Q}/\mathbb{Z}$.

Solution:

Proof. Any element α with finite order in the group necessarily has the form

$$\alpha = r + \mathbb{Z}$$

where we must be able to find a $k \in \mathbb{N}$ such that

$$kr \in \mathbb{Z}.$$

This happens only when $r \in \mathbb{Q}$, thus we now know the set of elements of finite order $S \subseteq \mathbb{Q}/\mathbb{Z}$. But we already knew from the previous problem that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. Thus $\mathbb{Q}/\mathbb{Z} \subseteq S$. Therefore $S = \mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$. □

22. Section 8.3: 32
A group H is said to be **finitely generated** if there is a finite subset S of H such that $H = \langle S \rangle$ (see Theorem 7.18). If N is a normal subgroup of a group G such that the groups N and G/N are finitely generated, prove that G is finitely generated.

Solution:

Proof. Let $N, G/N$ be finitely generated.

$$N = \langle n_1, \cdots, n_k \rangle, G/N = \langle Ng_1, \cdots, Ng_n \rangle$$

for any $g \in g_{x_i}N$, we know there exists $n \in N$ such that $g = g_{x_i}n$ and

$$g_{x_i}n = g_{x_i}n_1^{j_1} \cdot n_2^{j_2} \cdots n_k^{j_k}$$
$$g \in \langle g_1, \cdots, g_n, n_1, \cdots, n_k \rangle$$

thus G is finitely generated. □

23. If p is prime, prove every quotient group of $\mathbb{U}_p$ is cyclic.

Proof. By the primitive root theorem, $\mathbb{U}_n$ is cyclic if n is $1, 2, 4, p^k, 2p^k$. Thus $\mathbb{U}_p$, p prime, is cyclic. By problem 19, we know every quotient group G/N is also cyclic for any cyclic G is cyclic. □

24. Determine the lattice of ALL subgroups of A_4. Determine which of the subgroups are normal.

Solution:

A_4, $\{e, (12)(34), (13)(24), (14)(23)\}$ and the trivial group are normal. These are either verified easily. See Question 2 and Question 3.

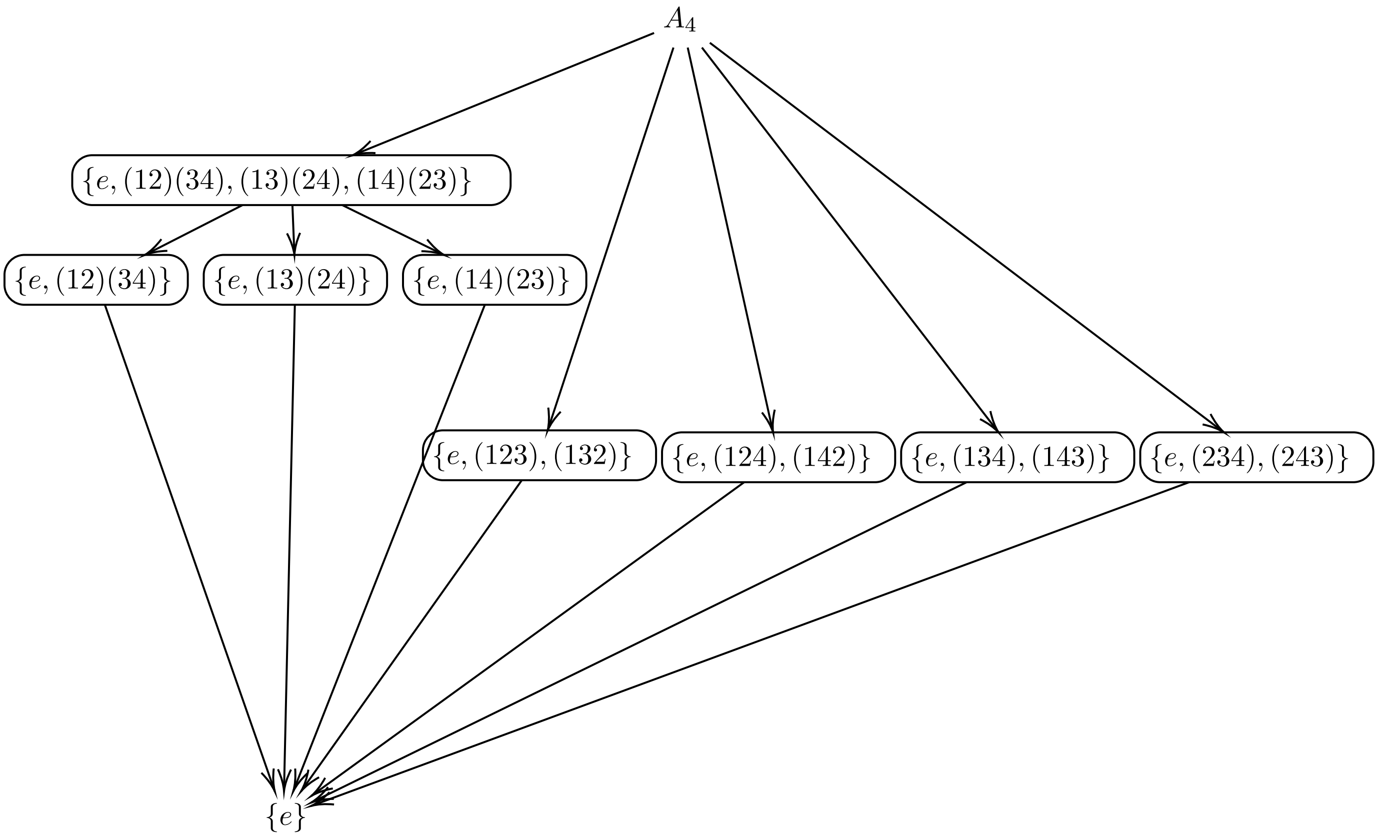

Figure 10: Subgroup Lattice

University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25th May, 2021
Zhewen Zheng

Homework 4

Problems to TURN IN

1. Section 7.1: 16

   Let **l,i,j,k** be the following matrices with complex entries

$$\mathbf{l} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

   (a) Prove that

$$\begin{aligned} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 &\qquad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i} &\qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j} \end{aligned}$$

Solution:

Proof.

$$\begin{aligned}
\mathbf{i}^2 &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
\mathbf{j}^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
\mathbf{k}^2 &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
\mathbf{i}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{l} \\
\mathbf{ij} &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\
\mathbf{ji} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\
\mathbf{ij} &= -\mathbf{ji} = \mathbf{k} \\
\mathbf{jk} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\
\mathbf{kj} &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \\
\mathbf{jk} &= -\mathbf{kj} = \mathbf{i} \\
\mathbf{ki} &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
\mathbf{ik} &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
\mathbf{ki} &= -\mathbf{ik} = \mathbf{j}
\end{aligned}$$

□

(b) Show that set $Q = \{\mathbf{l,i,\text{-}l,\text{-}i,j,k,\text{-}j,\text{-}k}\}$ is a group under matrix multiplication by writing out its multiplication table. Q is called the quaternion group.

Solution:

	l	**i**	**j**	**k**
l	**l**	**i**	**j**	**k**
i	**i**	**-l**	**k**	**-j**
j	**j**	**-k**	**-l**	**i**
k	**k**	**j**	**-i**	**-l**

2. Let Q be quaternion group in previous problem

(a) Determine all subgroups, normal subgroups and the lattice of subgroups for Q

Solution:

Order	Groups
1	$\{\mathbf{1}\}$
2	$\{\mathbf{1}, -\mathbf{1}\}$
4	$\{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}\}, \{\mathbf{1}, -\mathbf{1}, \mathbf{j}, -\mathbf{j}\}, \{\mathbf{1}, -\mathbf{1}, \mathbf{k}, -\mathbf{k}\}$
8	Q

In fact, all subgroups are normal; $\{\mathbf{1}\}$ is the trivial group, $\{\mathbf{1}, -\mathbf{1}\}$ is the center of Q thus is normal, and $\{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}\}, \{\mathbf{1}, -\mathbf{1}, \mathbf{j}, -\mathbf{j}\}, \{\mathbf{1}, -\mathbf{1}, \mathbf{k}, -\mathbf{k}\}$ all have index 2 which we know is normal.

(b) Determine the group structure of Q/N for all proper normal subgroups N of Q.

Solution:

Let $N = \{\mathbf{1}\}$

$$Q/N = Q$$

Let $N = \{\mathbf{1}, -\mathbf{1}\}$

$$\begin{aligned}[Q : N] &= 4 \\ Q/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ or } Q/N &\cong \mathbb{Z}_4\end{aligned}$$

Check the cosets

$$\begin{aligned}
N\mathbf{1} &= \{\mathbf{1}, -\mathbf{1}\} \\
N\mathbf{i} &= \{\mathbf{i}, -\mathbf{i}\} \\
N\mathbf{j} &= \{\mathbf{j}, -\mathbf{j}\} \\
N\mathbf{k} &= \{\mathbf{k}, -\mathbf{k}\} \\
Q/N &= \{N, N\mathbf{i}, N\mathbf{j}, N\mathbf{k}\} \\
\langle N \rangle &= N, |N| = 1 \\
N(\mathbf{i}^2) &= N(-\mathbf{1}) = N, |N\mathbf{i}| = 2 \\
N(\mathbf{j}^2) &= N(-\mathbf{1}) = N, |N\mathbf{j}| = 2 \\
N(\mathbf{k}^2) &= N(-\mathbf{1}) = N, |N\mathbf{k}|W = 2
\end{aligned}$$

Since Q/N has no element of order 4, by our classification result, $Q/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. WLOG Let $N = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}\}$. Then

$$\begin{aligned}[Q : N] &= 2 \\ Q/N &\cong \mathbb{Z}_2\end{aligned}$$

3. Section 8.4: 6
$h : \mathbb{C}^* \to \mathbb{C}^*$, where $h(x) = x^4$.

Solution:

- Homomorphism:

$$\begin{aligned} h(ab) &= (ab)^4 \\ &= (a^4b^4 \\ &= h(a)h(b) \end{aligned}$$

- Surjective: For any $a \in \mathbb{C}^*$, there is an element $b = \sqrt[4]{a} \in \mathbb{C}^*$ such that $h(\sqrt[4]{a}) = \sqrt[4]{a}^4 = a$.
- Kernel:

$$\begin{aligned} K &= \{g \in \mathbb{C}^* \mid h(g) = e_{\mathbb{C}^*}\} \\ &= \{g \in \mathbb{C}^* \mid g^4 = 1 + 0i\} \\ &= \{1, -1, i, -i\} \end{aligned}$$

4. Section 8.4: 12
$h : \mathbb{Z}_{12} \to \mathbb{Z}_6$, where $h([a]_{12}) = [a]_6$

Solution:

- Homomorphism:

$$\begin{aligned} h([ab]_{12}) &= [ab]_6 \\ &= [a]_6[b]_6 \\ &= h([a]_{12})h([b]_{12}) \end{aligned}$$

- Surjective: Since all elements $a \in \mathbb{Z}_6$ is also in $\mathbb{Z}_{12}$, we have for any element $[a]_6 \in \mathbb{Z}_6$, there exists $[a]_{12} \in \mathbb{Z}_{12}$ such that $h([a]_{12}) = [a]_6$.

5. Section 8.4: 18
Find all homomorphic images of D_4.

Solution:

The nontrivial proper normal subgroups of D_4 are: Order 4:

$$\{e, r, r^2, r^3\}, \{e, sr, r^2, sr^3\}, \{e, r^2, s, sr^2\}$$

Order 2:

$$\{e, r^2\}$$

For normal subgroups of order 4, let N be any such normal subgroup

$$\begin{aligned} [D_4 : N] &= 2 \\ D_4/N &\cong \mathbb{Z}_2 \end{aligned}$$

For normal subgroups of order 2, let $N = \{e, r^2\}$

$$[D_4 : N] = 4$$

$$D_4/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ or } D_4/N \cong \mathbb{Z}_4$$

Check the cosets

$$\begin{aligned}
Ne &= N \\
Nr &= \{r, r^3\} \\
Nr^2 &= \{r^2, e\} = N \\
Nr^3 &= \{r^3, r\} = Nr \\
Nd &= \{d, r^2 d\} \\
N(dr) &= \{rd, r^3 d\} \\
D_4 &= \{N, Nr, Nd, Ndr\} \\
|N| &= 1 \\
|Nr| &= 2 \\
|Nd| &= 2 \\
|Ndr| &= 2
\end{aligned}$$

Since D_4/N has no element of order 4, by our classification result, $D_4/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

6. Section 8.4: 19
   Find all homomorphic images of S_3.

   Solution:

   The only nontrivial proper normal subgroups of S_3 is A_3

   $$A_3 = \{e, (123), (132)\}$$

   For the subgroups with order 2, we can easily check that they are not normal. Let $N = A_3$.

   $$[S_3 : N] = 2$$

   Thus N is normal and $S_3/N \cong \mathbb{Z}_2$

7. Section 8.4: 20

   (a) List all subgroups of $\mathbb{Z}_{12}/H$, where $H = \{0, 6\}$.

   Solution:

   $$\begin{aligned}
   \mathbb{Z}_{12}/H &= \{H, H+1, H+2, H+3, H+4, H+5\} \\
   \langle H+1 \rangle &= \langle H+5 \rangle = \mathbb{Z}_{12}/H \\
   \langle H+2 \rangle &= \langle H+4 \rangle = \{H, H+2, H+4\} \\
   \langle H+3 \rangle &= \{H, H+3\}
   \end{aligned}$$

   Thus the subgroups are

   $$\{H\}, \{H, H+3\}, \{H, H+2, H+4\}, \mathbb{Z}_{12}/H$$

(b) List all subgroups of $\mathbb{Z}_{20}/K$, where $K = \{0, 4, 8, 12, 16\}$.

Solution:

$$\begin{aligned} \mathbb{Z}_{20}/H &= \{H, H+1, H+2, H+3\} \\ \langle H+1 \rangle &= \{H, H+1, H+2, H+3\} \\ \langle H+2 \rangle &= \{H, H+2\} \\ \langle H+3 \rangle &= \{H, H+1, H+2, H+3\} \end{aligned}$$

Thus the subgroups are

$$\{H\}, \{H, H+2\}, \mathbb{Z}_{20}/H$$

8. Section 8.4: 22
Let G be an abelian group.

(a) Show that $K = \{a \in G \mid |a| \leq 2\}$ is a subgroup of G.

Solution:

Proof. Since $K = \{a \in G \mid |a| \leq 2\}$,

$$K = \{a \in G \mid a^2 = e\}$$

Let $a, b \in K$. Then

$$(ab)^2 = a^2b^2 = e$$

thus $ab \in K$. Also since for any $a \in K$, because $|a| \leq 2$, we have $a^{-1} \in K$. Thus K is a subgroup of G. □

(b) Show that $H = \{x^2 \mid x \in G\}$ is a subgroup of G.

Solution:

Proof. Let $a^2, b^2 \in H, a, b \in G$.

$$a^2b^2 = (ab)^2 \in H$$

Also,

$$(a^2)^{-1} = (a^{-1})^2 \in H$$

Thus H is a subgroup of G. □

(c) Prove that $G/K \cong H$. [Hint: Define a surjective homomorphism from G to H with kernel K.]

Solution:

Proof. Consider $f : G \to H, f(g) = g^2 \in H$.

i. Homomorphism: Let $a, b \in G$

$$\begin{aligned} f(ab) &= (ab)^2 \\ &= a^2b^2 \\ &= f(a)f(b) \end{aligned}$$

ii. Surjective: By definition, for any $b^2 \in H$, there is a $b \in G$ such that $f(b) = b^2$.

We can check the $\ker f$:

$$K = \{a \in G \mid a^2 = e\} = \{a \in G \mid |a| \leq 2\}$$

Now, by the First Isomorphism Theorem, since we have a surjective homomorphism $f : G \to H$ with kernel K, we therefore have $G/K \cong H$. □

9. Section 8.4: 24
If $k \mid n$ and $f : \mathbb{U}_n \to \mathbb{U}_k$ is given by $f([x]_n) = [x]_k$, show that f is a homomorphism and find its kernel.

Solution:

(a) Well-defined: Let $[x]_n = [y]_n \in \mathbb{U}_n$. Then

$$\begin{aligned} x &\equiv y \mod n \\ n &\mid (x - y) \\ k &\mid (x - y) \\ x &\equiv y \mod k \\ [x]_k &= [y]_k \in \mathbb{U}_k \end{aligned}$$

(b) Homomorphism:

$$\begin{aligned} f([x]_n[y]_n) &= f([xy]_n) \\ &= [xy]_k \\ &= [x]_k[y]_k \\ &= f([x]_n)f([y]_n) \end{aligned}$$

(c) Kernel:

$$K = \ker f = \{x \in \mathbb{U}_n \mid f(x) = [1]_k\} = \{x \in \mathbb{U}_n \mid x \equiv 1 \mod k\}$$

10. Section 8.4: 28
$SL(2, \mathbb{R})$ is a normal subgroup of $GL(2, \mathbb{R})$ by Exercise 25 of Section 8.2. Prove that $GL(2, \mathbb{R})/SL(2, \mathbb{R})$ is isomorphic to the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

Solution:

Proof. Let $f : GL(2,\mathbb{R}) \to \mathbb{R}^*, f(A) = \det A$.

(a) Homomorphism: Let $A, B \in GL(2,\mathbb{R})$

$$\begin{aligned} f(AB) &= \det(AB) \\ &= \det A \det B \\ &= f(A)f(B) \end{aligned}$$

(b) Surjective: for any $r \in \mathbb{R}^*$, there exists $ab - cd = r, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $\det A = ab - cd = r$.

(c) Kernel:

$$K = \{A \in GL(2,\mathbb{R}) \mid f(A) = 1\} = \{A \in GL(2,\mathbb{R}) \mid \det(A) = 1\}$$

by definition $K = SL(2,\mathbb{R})$. Now, by the First Isomorphism Theorem,

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) \cong \mathbb{R}^*$$

□

11. Section 8.4: 37
Prove that $\mathbb{Q}^* \cong \mathbb{Q}^{**} \times \mathbb{Z}_2$. [Hint: Exercises 4 and 36.]

Solution:

Proof. $\mathbb{Q}^{**}$ is a subgroup of $\mathbb{Q}^*$; Let $a, b \in \mathbb{Q}^{**}$. Then $ab \in \mathbb{Q}^{**}$. Since Q^* is abelian, $\mathbb{Q}^{**}$ is normal. We can have the homomorphism $f : \mathbb{Q}^* \to \mathbb{Q}^{**}, f(x) = |x|$ from exercise 4. Then we can restrict f to $\mathbb{Q}^{**}$ so that f becomes an automorphism and $\mathbb{Q}^{**} \cong \mathbb{Q}^{**}$. Now we check the kernel of f:

$$K = \{-1, 1\}$$

By our classification theorem, $K \cong \mathbb{Z}_2$. Thus by Exercise 36, $\mathbb{Q}^* \cong \mathbb{Q}^{**} \times \mathbb{Z}_2$. □

12. Section 8.4: 38
Let N be a normal subgroup of a group G. Prove that G/N is simple if and only if there is no normal subgroup K such that $N \subsetneq K \subsetneq G$. [Hint: Corollary 8.23 and Theorem 8.24.]

Solution:

Proof. $\Longrightarrow$ Let G/N be simple. If there is a normal subgroup K such that $N \subseteq K \subseteq G$, then by the Third Isomorphism Theorem, K/N is a normal subgroup of G/N. Since G/N is simple, it must be $K/N = \{e\}$ or $K/N = G/N$, which means $K = N$ or $K = G$. Thus there is no normal subgroup K such that $N \subsetneq K \subsetneq G$.

$\Longleftarrow$ Let there be no normal subgroup K such that $N \subsetneq K \subseteq G$. This means any normal subgroup K either has $K = N$ or $K = G$. This implies $K/N = \{e\}$ or $K/N = G/N$. Thus the only possible normal subgroups of G/N given by Corollary 8.23 are $\{e\}, G/N$. Thus G/N is simple.

□

13. Section 8.4: 40 **(Second Isomorphism Theorem)** Let K and N be subgroups of a group G, with N normal in G. Then $NK = \{nk \mid n \in N, k \in K\}$ is a subgroup of G that contains both K and N by Exercise 20 of Section 8.2.

(a) Prove that N is a normal subgroup of NK.

Solution:

Proof. Since N is normal in G, we have $g^{-1}Ng = N$ for all $g \in G$, and in particular we also have $g^{-1}Ng = N$ for $g \in NK \subset G$. Thus N is normal in G. □

(b) Prove that the function $f : K \to NK/N$ given by $f(k) = Nk$ is a surjective homomorphism with kernel $K \cap N$.

Solution:

Proof. i. Homomorphism:

$$\begin{aligned} f(ab) &= Nab \\ &= (Na)(Nb) \\ &= f(a)f(b) \end{aligned}$$

ii. Surjective: Let $g \in NK$. Then $g = nk$ for some $n \in N, k \in K$. Then

$$\begin{aligned} Ng &= N(nk) \\ &= Nk = f(k) \end{aligned}$$

iii. Kernel:

$$K = \{k \in K \mid f(k) = N\} = \{k \in K \mid Nk = N\}$$

This equivalent to $k \in K \cap N$. Thus

$$K = \{k \in K \mid k \in K \cap N\}.$$

□

(c) Conclude that $K/(N \cap K) \cong NK/N$.

Solution:

By the First Isomorphism Theorem, $G/(K \cap N) \cong NK/N$.

14. Section 8.5: 4
If $n \geq 5$, what is the center of A_n?

Solution:

The center of A_n is just $\{e\}$ since all $A_n, n \neq 4$ are simple.

15. Section 8.5: 8
Prove that no subgroup of order 2 in $S_n (n \geq 3)$ is normal. [Hint: Exercises 26 of Section 7.5 and 16 of Section 8.2.]

Solution:

Proof. By Exercise 26 of Section 7.5, the center of $S_n (n \geq 3)$ is the identity subgroup. Also, Exercise 16 of Section 8.2, if we have a normal subgroup K of order 2, we must have $K \subseteq Z(S_n(n \geq 3)$. But then it's impossible for K to have order 2 and $K \subseteq \{e\}$. Therefore no subgroup of order 2 in $S_n (n \geq 3)$ is normal. □

16. Section 8.5: 10
If N is a normal subgroup of S_n and $N \cap A_n = A_n$, prove that $N = A_n$ or S_n. [Hint: Why is $A_n \subseteq N \subseteq S_n$? Use Theorem 7.29 and Lagrange's Theorem.]

Solution:

Proof. Since we have $N \cap A_n = A_n$, this means that for all $x \in N$ and $x \in A_n$, $x \in A_n$. In particular for all $x \in N$ we have $x \in A_n$. Thus $A_n \subseteq N$. Since N is a subgroup of S_n, $N \subseteq S_n$. Thus $A_n \subseteq N \subseteq S_n$. Now, by Lagrange's Theorem, $|N| \mid |S_n|$. However, we also have $|S_n| = n!, |A_n| = \frac{n!}{2}, |S_n|/|A_n| = 2$, which means we should have $|S_n|/|N| \leq 2$. If $|S_n|/|N| = 1$, then $N = S_n$. If $|S_n|/|N| = 2$, then $N = A_n$. □

17. Section 8.5: 12
If $f : S_n \to S_n$ is a homomorphism, prove that $f(A_n) \subseteq A_n$.

Solution:

Proof. By Corollary 8.29, for $n \geq 5$ the only normal subgroups for S_n is $(1), A_n, S_n$. If $\ker f = (1)$ then f is an isomorphism; thus $f(A_n) \cong A_n \subseteq A_n$. If $A_n \subseteq \ker f$, which means $\ker f = S_n$ or $\ker f = A_n$, then $f(A_n) = (1) \subseteq A_n$. □

18. Section 9.1: 2
What is the order of the group $\mathbb{U}_5 \times \mathbb{U}_6 \times \mathbb{U}_7 \times \mathbb{U}_8$?

Solution:

$$|\mathbb{U}_5 \times \mathbb{U}_6 \times \mathbb{U}_7 \times \mathbb{U}_8| = |\mathbb{U}_5||\mathbb{U}_6||\mathbb{U}_7||\mathbb{U}_8| = 4 \cdot 2 \cdot 6 \cdot 4 = 192$$

19. Section 9.1: 18
Prove that $\mathbb{U}_{16}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. [Hint: Theorem 9.3]

Solution:

Proof.

$$\begin{aligned}
\mathbb{U}_{16} &= \{1,3,5,7,9,11,13,15\} \\
\langle 3 \rangle &= \{1,3,9,13\} \\
\langle 7 \rangle &= \{1,7\} \\
\langle 3 \rangle \cong \mathbb{Z}_4, \langle 7 \rangle &\cong \mathbb{Z}_2 \\
\langle 3 \rangle \langle 7 \rangle &= \{1,3,5,7,9,11,13,15\} = \mathbb{U}_{16} \\
\mathbb{Z}_2 \cap \mathbb{Z}_4 &= \{e\}
\end{aligned}$$

By Theorem 9.3

$$\begin{aligned}
\langle 3 \rangle \times \langle 7 \rangle &= \mathbb{U}_{16} \\
\mathbb{Z}_2 \times \mathbb{Z}_4 \cong \langle 3 \rangle \times \langle 7 \rangle &= \mathbb{U}_{16}
\end{aligned}$$

□

20. Section 9.1: 22
Let G and H be finite cyclic groups. Prove that $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Solution:

Proof. Let $g \in G, h \in H, |g| = |G| = m, |h| = |H| = n$ where $\langle g \rangle = G, \langle h \rangle = H$. We have $(g,h) \in G \times H$. Let $l = \text{lcm}(m,n)$. Thus $l = \alpha m = \beta n$. Notice

$$(g,h)^l = (g^{\alpha m}, h^{\beta n}) = (e_G, e_H) = e_{G \times H}.$$

We see that $|(g,h)| = \text{lcm}(m,n)$. Now, if $G \times H$ is cyclic, then $|G \times H| = mn$ and we must have an element of order mn. Thus we must have $\text{lcm}(m,n) = mn$. If $\text{lcm}(m,n) = mn$ then $(m,n) = 1$. Now the other direction: If $(m,n) = 1$, then $\text{lcm}(m,n) = mn$, which means there is an element k of order mn in $G \times H$. This means $G \times H$ is generated by k and thus is cyclic. □

21. Section 9.1: 36
If $(m,n) = 1$, prove that $\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$.

Solution:

Proof. Let $f : \mathbb{U}_{mn} \to \mathbb{U}_m \times \mathbb{U}_n, f([a]_{mn}) = ([a]_m, [a]_n)$.

(a) Homomorphism:

$$\begin{aligned} f([a]_{mn}[b]_{mn}) &= f([ab]_m n) \\ &= ([ab]_m, [ab]_n) \\ &= ([a]_m, [a]_n)([b]_m, [b]_n) \\ &= f([a]_{mn})f([b]_{mn}) \end{aligned}$$

(b) Injective: Let elements $([a]_m, [a]_n), ([b]_m, [b]_n) \in \mathbb{U}_m \times \mathbb{U}_n$. If $([a]_m, [a]_n) = ([b]_m, [b]_n)$ then we have

$$m \mid a - b \text{ and } n \mid a - b$$

thus

$$mn \mid a - b$$

and thus $[a]_{mn} = [b]_{mn} \in \mathbb{U}_{mn}$. Thus injective.

(c) Surjective: Since this is finite and the domain and range has same cardinality and f is injective, f is surjective. Therefore $\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$. Alternatively we could allude to the fact that given $(m, n) = 1$

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$$

and the units also had the isomorphism .

□

22. As in example 3 on page 285, write $\mathbb{U}_n$ as both an internal direct product of cyclic groups and as an external direct product of $\mathbb{Z}_k$'s in these three cases

(a) $\mathbb{U}_{32}$

Solution:

$$\begin{aligned} \mathbb{U}_{32} &= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\} \\ M &= \langle 3 \rangle = \{1, 3, 9, 11, 17, 19, 25, 27\} \\ N &= \langle 15 \rangle = \{1, 15\} \\ M \cap N &= 1 \end{aligned}$$

We know that $M < MN$, and $|M| = 8$. So by Lagrange $|MN| = 16$ and

$$\begin{aligned} MN &= \mathbb{U}_{32} \\ \mathbb{U}_{32} &\cong \langle 3\rangle \times \langle 15\rangle \end{aligned}$$

Also,

$$\begin{aligned} \langle 3\rangle \cong \mathbb{Z}_8 \quad \langle 15\rangle &\cong \mathbb{Z}_2 \\ \mathbb{U}_{32} &\cong \mathbb{Z}_8 \times \mathbb{Z}_2 \end{aligned}$$

(b) $\mathbb{U}_{55}$

Solution:

Since $(5, 11) = 1$,

$$\mathbb{U}_{55} \cong \mathbb{U}_5 \times \mathbb{U}_{11}$$

Since $\mathbb{U}_5 \cong \mathbb{Z}_4$ and $\mathbb{U}_{11} \cong \mathbb{Z}_{10}$, we have

$$\mathbb{U}_{55} \cong \mathbb{Z}_4 \times \mathbb{Z}_{10} \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \cong \mathbb{Z}_{20} \times \mathbb{Z}_2$$

Also note

$$\begin{aligned} M &= \langle 2\rangle = \{1, 2, 4, 8, 16, 32, 9, 18, 36, 17, 34, 13, 26, 52, 49, 43, 31, 7, 14, 28\} \\ N &= \langle 21\rangle = \{1, 21\} \\ M \cap N &= \{1\} \end{aligned}$$

Since $M < MN$ and $|M| = 20$, by Lagrange $|MN| = 40$ and thus

$$\begin{aligned} MN &= \mathbb{U}_{55} \\ \mathbb{U}_{55} &\cong \langle 2\rangle \times \langle 21\rangle \end{aligned}$$

(c) $\mathbb{U}_{140}$

Solution:

Because $140 = 7 \cdot 20, (7, 20) = 1$, we have

$$\mathbb{U}_{140} \cong \mathbb{U}_7 \times \mathbb{U}_{20} \cong \mathbb{Z}_6 \times \mathbb{Z}_8 \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$\begin{aligned} M &= \langle 41\rangle = \{1, 41\} \\ N &= \langle 13\rangle = \{1, 13, 29, 97\} \\ L &= \langle 11\rangle = \{1, 11, 121, 71, 81, 51\} \\ \langle 41\rangle \cap \langle 13\rangle \cap \langle 11\rangle &= \{1\} \end{aligned}$$

Since

$$\begin{aligned} \langle 41\rangle &\cong \mathbb{Z}_2 \\ \langle 13\rangle &\cong \mathbb{Z}_4 \\ \langle 11\rangle &\cong \mathbb{Z}_6 \end{aligned}$$

note

$$L < NL, |NL| < |\mathbb{U}_{140}|, |NL| = 12 \text{ or } |NL| = 24.$$

Suppose $N' = N \times L$. We know that $N' \cong \mathbb{Z}_4 \times \mathbb{Z}_6, N \cap L = \{1\}$. Clearly $N' = NL, |NL| = 24$. Now, $N' < MN'$ and thus by Lagrange we have $|MN'| = 48$, which means

$$\mathbb{U}_{140} \cong M \times N' \cong \mathbb{M} \times N \times L \cong \langle 41 \rangle \times \langle 13 \rangle \times \langle 11 \rangle$$

23. Section 9.2: 3(b,d,f,h)
List all abelian groups (up to isomorphism) of the given order:
(b) 15 (d) 72 (f) 144 (h) 1160

Solution:

Order	Abelian Groups
15	$\mathbb{Z}_3 \oplus \mathbb{Z}_5$
72	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$
	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_8 \oplus \mathbb{Z}_9$
144	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$
	$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9$
	$\mathbb{Z}_{16} \oplus \mathbb{Z}_3\mathbb{Z}_3$
	$\mathbb{Z}_{16} \oplus \mathbb{Z}_9$
1160	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29}$
	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29}$
	$\mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{29}$

24. Section 9.2: 5(b,d)
Find the elementary divisors of the given group:
(b) $\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ (d) $\mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{100} \oplus \mathbb{Z}_{240}$

Solution:

Group	Elementary Divisors
$\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$	$2, 2, 2^2, 3, 3, 3^2$
$\mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{100} \oplus \mathbb{Z}_{240}$	$2, 2^2, 2^2, 2^4, 3, 3, 3, 5, 5, 5^2$

25. Section 9.2: 6
Find the invariant factors of each of the groups in Exercise 5.

Solution:

Group	Invariant Factors
$\mathbb{Z}_{250}$	250
$\mathbb{Z}_6 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$	$6, 6, 36$
$\mathbb{Z}_{10} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{30}$	$2, 10, 20, 40$
$\mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{100} \oplus \mathbb{Z}_{240}$	$2, 60, 60, 1200$

26. Section 9.2: 8
If G is the additive group $\mathbb{Q}/\mathbb{Z}$, what are the elements of the subgroup $G(2)$? Of $G(p)$ for any positive prime p?

Solution:

Elements in $G(2)$ are of the form $n/2^k + \mathbb{Z}$ for some $k \geq 0$. Elements in $G(p)$ are of the form $n/p^k + \mathbb{Z}$ for some $k \geq 0$.

27. Section 9.2: 12
Cauchy's Theorem for Abelian Group If G is a finite abelian group and p is a prime that divides $|G|$, prove that G contains an element of order p. [Hint: Use the Fundamental Theorem to show that G has a cyclic subgroup of order p^k; use Theorem 7.9 to find an element of order p.]

Solution:

Proof. First, by the Fundamental Theorem of Finite Abelian Groups, G is the direct sum of cyclic groups, each of prime order. These cyclic groups are subgroups of G (Since they are subgroups of $G(p)$ and $G(p)$s are subgroups of G). Thus there G has a cyclic subgroup of order p^k for some $k \geq 0$. Then, By Theorem 7.9,

$$pa = 0 \iff p \mid p^k$$

Thus there exists an element a with order p. □

28. Section 9.2: 13
Prove that a finite abelian p-group has order a power of p.

Solution:

Proof. Suppose we have a finite abelian p-group that does not have a order of a power of p. Then $|G| \neq p^k$ for all $k \geq 0$. Then $q \mid |G|$ for some other prime $q \neq p$. By Cauchy's Theorem for Abelian Group, G has an element of order q, which contradicts our definition of p-groups. Thus a finite abelian p-group has order a power of p. □

29. Section 9.2: 16
For which positive integers n is there exactly one abelian group of order n (up to isomorphism)?

Solution:

Either $n = 1$ or $n = p_1 \cdots p_k$ where each p_i for $1 \leq i \leq k$ are distinct primes. This is because once we have a power of a prime, then we introduce additional elementary divisors which correspond to other abelian group of order n that is not isomorphic to the one we had already constructed.

University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25th May, 2021
Zhewen Zheng

Homework 5

Problems to TURN IN

1. Let $\phi(n)$ be the number of positive integers less than n relatively prime to n. This is called the Euler Phi Function. By Math 402 work, notice that $|\mathbb{U}_n| = \phi(n)$. An elementary number theory class typically describes how to efficiently compute $\phi(n)$. However, this exercise will show how to obtain those same results using the group theory work in Lecture 19.

   (a) Prove: If p is prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. (You can prove this directly by counting things NOT relatively prime to p^k.)

   Solution:

   Proof. Since p prime, if we have m such that $\gcd(m, p^k) > 1$, then $m = lp$ for some $1 \leq l \leq p^{k-1}$. Since we can find p^{k-1} choices of l, there are p^{k-1} elements not relatively prime to p^k. Thus we have $p^k - p^{k-1}$ numbers relatively prime to p^k

   $$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

   □

   (b) Using the work in Lecture 19, Prove: If $\gcd(a,b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. (This is the famous "Phi function multiplicativity Theorem").

   Solution:

   Proof. In Lecture 19 we have shown that when $\gcd(a,b) = 1$,

   $$\mathbb{U}_{ab} \cong \mathbb{U}_a \times \mathbb{U}_b$$

   Since we know that the order of a direct product is the product of the orders,

   $$|\mathbb{U}_{ab}| = |\mathbb{U}_a \times \mathbb{U}_b|$$
   $$|\mathbb{U}_{ab}| = |\mathbb{U}_a||\mathbb{U}_b|$$

   And by the definition of the Euler Phi Function and $\mathbb{U}_n$ groups,

   $$\phi(ab) = |\mathbb{U}_{ab}| = |\mathbb{U}_a||\mathbb{U}_b| = \phi(a)\phi(b)$$

   □

   (c) Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the factorization of n into distinct prime powers. Prove:

   $$\phi(n) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1).$$

Solution:

Proof. Let n the same as stated in the prompt. In Lecture 19 we have shown that

$$\mathbb{U}_n \cong \mathbb{U}_{p_1^{k_1}} \times \cdots \mathbb{U}_{p_r^{k_r}}$$

Since we know that the order of a direct product is the product of the orders,

$$\begin{aligned} |\mathbb{U}_n| &= \left|\mathbb{U}_{p_1^{k_1}} \times \cdots \mathbb{U}_{p_r^{k_r}}\right| \\ &= \prod_{i=1}^{r} \left|\mathbb{U}_{p_i^{k_i}}\right| \end{aligned}$$

And by the definition of the Euler Phi Function and $\mathbb{U}_n$ groups with (a),

$$\phi(n) = |\mathbb{U}_n| = \prod_{i=1}^{r} \left|\mathbb{U}_{p_i^{k_i}}\right| = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1)$$

□

(d) What is the order of the group $\mathbb{U}_{945000}$?

Solution:

$$\begin{aligned} 945000 &= 2^3 3^3 5^4 7^1 \\ \mathbb{U}_{945000} &\cong \mathbb{U}_{2^3} \times \mathbb{U}_{3^3} \times \mathbb{U}_{5^4} \times \mathbb{U}_7 \\ |\mathbb{U}_{945000}| &= \phi(2^3)\phi(3^3)\phi(5^4)\phi(7) \\ &= (2^2(2-1))(3^2(3-1))(5^3(5-1))(7^0(7-1)) \\ &= 216000 \end{aligned}$$

2. Let p be an odd prime integer and $k \geq 2$. Prove: $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \mod p^k$.

Solution:

Proof.

$$(1+p)^{p^{k-2}} = \sum_{l=0}^{p^{k-2}} \binom{p^{k-2}}{l} p^l$$

Let $c_l = \binom{p^{k-2}}{l}$. Let's analyze the coefficients:

$$\begin{aligned} c_0 &= \binom{p^{k-2}}{0} = 1 \\ c_1 &= \binom{p^{k-2}}{1} = \frac{p^{k-2}!}{1!\,(p^{k-2}-1)!} = p^{k-2} \\ c_2 &= \binom{p^{k-2}}{2} = \frac{p^{k-2}!}{2!\,(p^{k-2}-2)!} = \frac{p^{k-2}\left(p^{k-2}-1\right)}{2!} = p^{k-2}\,\frac{\overbrace{p^{k-2}}^{\alpha}}{2!} \end{aligned}$$

Notice now that

$$\begin{aligned}(1+p)^{p^{k-2}} &= 1 + p^{k-2}p + \alpha p^{k-2}p^2 + \cdots + p^{p^{k-2}} \\ &= 1 + p^{k-1} + \alpha p^k + \cdots + p^k p^t\end{aligned}$$

where $k + t = p^{k-2}$. Now

$$\begin{aligned}(1+p)^{p^{k-2}} &= 1 + p^{k-1} + \alpha p^k + \cdots + p^k p^t \\ (1+p)^{p^{k-2}} - (1+p^{k-1}) &= \alpha p^k + \cdots + p^k p^t \\ p^k &\mid (1+p)^{p^{k-2}} - (1+p^{k-1}) \\ (1+p)^{p^{k-2}} &\equiv \left(1 + p^{k-1}\right) \mod p^k\end{aligned}$$

□

3. Follow the proof of the $\mathbb{U}_n$ decomposition theorem from Lecture 19 to explicitly produce an internal direction product of cyclic subgroups:

$$\mathbb{U}_{p^n} \cong \langle x \rangle \times \langle y \rangle$$

in these cases: (a) $p = 7, n = 3$; (b) $p = 2, n = 5$

Solution:

(a) From Lecture 19 we know that we need an x such that $x = a^{p^{n-1}}$, where a is a generator of $\mathbb{U}_{p^n}$. That means we need to find a such that

$$a^{p-1} \equiv 1 \mod p \text{ and } a^l \not\equiv 1 \mod p \text{ for } l < p - 1$$

Consider $a = 3$.

$$3^6 \equiv 1 \mod 7 \text{ and } 3^l \not\equiv 1 \mod 7 \text{ for } l < 6$$

Thus we have $x = 3^{7^{3-1}} \mod 343 = 325$. Then by Lecture 19 we find $y = p + 1 = 8$. Then

$$\mathbb{U}_{343} \cong \langle 325 \rangle \times \langle 8 \rangle$$

(b) From Lecture 19 we know that since p is even, we need to find an a such that

$$|a| = 2, a \notin \langle 3 \rangle$$

Consider $a = 7$

$$|15| = 2, 15 \notin \langle 3 \rangle$$

Then we know that

$$\mathbb{U}_{2^5} \cong \langle 15 \rangle \times \langle 3 \rangle$$

4. Lecture 20 supplement: 5.1.3
The symmetric group S_n acts naturally on the set $\{1, 2, \cdots, n\}$. Let $\sigma \in S_n$. Show that the cycle decomposition of σ can be recovered by considering the orbits of the action of the cyclic subgroup $\langle \sigma \rangle$ on $\{1, 2, \cdots, n\}$.

Solution:

We want $\langle\sigma\rangle$ act on $X = \{1, 2, \cdots, n\}$. If we take a look at the orbits, we see

$$\mathcal{O}(x) = \{\sigma^k x \mid \sigma^k \in \langle\sigma\rangle\} \text{ for some integer power } k$$

Suppose the cycle decomposition of σ is $\sigma = \sigma_1\sigma_2\cdots\sigma_n$. Since the cycles are disjoint, there is only one cycle where $\sigma_i x \neq x$ and by Theorem 7.23 we can change the order of σ_i for $1 <\leq i \leq n$ since they are disjoint,

$$\sigma^k x = \sigma_i^k x$$

where i is unique. Observe that the orbit of x is the entire permutation cycle of x. Thus far, we are able to recover one disjoint cycle within σ. By finding the orbits of other elements in X which are different from the existing ones, we can repeatedly recover disjoint cycles σ_i for all i where $1 \leq i \leq n$.

5. Lecture 20 supplement: 5.1.5
Verify that any group G acts on the set X of its subgroups by $c_g(H) = gHg^{-1}$. Compute the example of S_3 acting by conjugation of the set X of (six) subgroups of S_3. Verify that there are four orbits, three of which consists of single subgroup, and one of which contains three subgroups.

Solution:

Let

$$\begin{aligned} c : G \to S(X), X = \{H_1, H_2\cdots\}, H_i \leq G \\ c_g(H) = gHg^{-1} \end{aligned}$$

Check homomorphism:

$$\begin{aligned} c_{gh}(H) &= (gh)H(gh)^{-1} \\ c_g(c_h(H)) &= c_g(hHh^{-1}) \\ &= ghHh^{-1}g^{-1} \\ &= (gh)H(gh)^{-1} \end{aligned}$$

For S_3, $X = \{S_3, \{e, (123), (132)\}, \{e, (12)\}, \{e, (23)\}, \{e, 13\}, \{e\}\}$. Then Let $H = S_3$

$$\mathcal{O}_H = S_3$$

Let $H = \{e, (123), (132)\} = A_3$

$$\mathcal{O}_H = \{gHg^{-1} \mid g \in S_3\} = A_3$$

Let $H = \{e, (12)\}$ or $\{e, (23)\}$ or $\{e, (13)\}$

$$\mathcal{O}_H = \{gHg^{-1} \mid g \in S_3\} = \{\{e, (12)\}, \{e, (23)\}, \{e, (13)\}\}$$

Let $H = \{e\}$

$$\mathcal{O}_H = \{e\}$$

6. Lecture 20 supplement: 5.1.6
Let G act on X, and let $x \in X$. Verify that Stab(x) is a subgroup of G. Verify that if x and y are in the same orbit, then the subgroups Stab(x) and Stab(y) are conjugate subgroups.

Solution:

Notice $e \in \text{Stab}(x)$. Thus $\text{Stab}(x)$ is not empty. Let $g, h \in \text{Stab}(x)$. Then $g \in G, ax = x$ and $h \in G, hx = x$.

$$\begin{aligned}(gh)x &= g(hx) \\ &= gx \\ &= x\end{aligned}$$

Thus $gh \in \text{Stab}(x)$. Also,

$$\begin{aligned}x &= (g^{-1}g)x \\ &= g^{-1}(gx) \\ &= g^{-1}x\end{aligned}$$

which gives us $g^{-1} \in \text{Stab}(x)$. Thus $\text{Stab}(x)$ is a subgroup of G.
Let $x, y \in X$ such that they are in the same orbit. Then $x, y \in \mathcal{O}(x)$. Thus

$$gx = y$$

Consider $\phi : \text{Stab}(x) \to \text{Stab}(y), \phi(a) = gag^{-1}$, Let $h \in \text{Stab}(x)$. Well-defined:

$$\begin{aligned}hx &= x \\ \phi(h)y &= ghg^{-1}y \\ &= ghx \\ &= gx \\ &= x\end{aligned}$$

Homomorphism:

$$\begin{aligned}\phi(hl) &= g(hl)g^{-1} \\ &= ghg^{-1}glg^{-1} \\ &= \phi(h)\phi(l)\end{aligned}$$

Injective:

$$\begin{aligned}\phi(h) &= \phi(l) \\ ghg^{-1} &= glg^{-1} \\ gh &= gl \\ h &= l\end{aligned}$$

Surjective: Let $k \in \text{Stab}(y)$.

$$\begin{aligned}ky &= y \\ k(gx) &= gx \\ g^{-1}kgx &= x \\ g^{-1}kg &\in \text{Stab}(x) \\ \phi(g^{-1}kg) &= gg^{-1}kgg^{-1} \\ &= k\end{aligned}$$

Thus bijective and Stab(x) and Stab(y) are conjugate subgroups.

7. Lecture 20 supplement: 5.1.7
Let $H = \{e, (1,2)\} \subseteq S_3$. Find the orbit of H under conjugation by G, the stabilizer of H in G, and the family of left cosets of the stabilizer in G, and verify explicitly the bijection between left cosets of the stabilizer and conjugates of H.

Solution:

$$\begin{aligned}\mathcal{O}_H &= \{gHg^{-1} \mid g \in G\} \\ &= \{\{e, (1,2)\}, \{e, (2,3)\}, \{e, (1,3)\}\} \\ G_H &= \{g \in G \mid gH = H\} \\ &= \{e, (1,2)\} \\ L &= \{aG_H \mid a \in G\} \\ &= \{\{e, (1,2)\}, \{(2,3), (1,2,3)\}, \{(1,3), (1,3,2)\}\}\end{aligned}$$

Notice that indeed the left cosets of the stabilizer and conjugates of H are one to one.

8. Prove: Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if σ and τ have the same disjoint cycle partition type.

Proof. $\Longrightarrow$ Let ρ be a permutation such that

$$\tau = \rho\sigma\rho^{-1}$$

and let $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$ be a disjoint cycle decomposition. Then

$$\tau = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1}) \cdots (\rho\sigma_k\rho^{-1})$$

since we know that the conjugate of a cycle has the same length as the cycle itself,

$$\text{CycleType}(\rho\sigma_i\rho^{-1}) = \text{CycleType}(\sigma_i)$$

Notice ρ is a bijection so $\rho\sigma_i\rho^{-1}$ are disjoint for $1 \leq i \leq k$. Therefore τ is expressed in a product of disjoint cycles which is the same partition type as σ.
$\Longleftarrow$ For this direction, since σ and τ has the same disjoint cycle partition type, we have

$$\begin{aligned}\sigma &= \sigma_1 \cdots \sigma_k \\ \tau &= \tau_1 \cdots \tau_k\end{aligned}$$

where σ_i and τ_i has the same cycle length for $1 \leq i \leq k$. Then consider a bijection(clear since they have same size) from $\sigma_i \to \tau_i$

$$\begin{aligned}\sigma_i &= (x_1, x_2, \cdots, x_l) \\ \tau_i &= (y_1, y_2, \cdots, y_l) \\ \rho(x_j) &= y_j, 1 \leq j \leq l\end{aligned}$$

Thus

$$\begin{aligned}\rho\sigma_i\rho^{-1}(y_j) &= \rho\sigma_i(x_j)\\ &= \rho x_{j+1}\\ &= y_{j+1}\\ &= \tau_i(y_j)\end{aligned}$$

for all x_i, y_i. Thus

$$\begin{aligned}\rho\sigma_i\rho^{-1} &= \tau_i\\ (\rho\sigma_1\rho^{-1})\cdots(\rho\sigma_k\rho^{-1}) &= \tau_i\cdots\tau_k\\ \rho\sigma\rho^{-1} &= \tau\end{aligned}$$

and thus σ and τ are conjugate. □

9. Let S_4 act on S_4 by conjugation and write down explicitly the orbits, which are the S_4-conjugacy classes (just use the previous problem). On the other hand, let A_4 act on S_4 by conjugation and write down explicitly the orbits, which would by the A_4-conjugacy classes.

Solution:

$$\begin{aligned}\mathcal{O}_{1,1,1,1} &= \{e\}\\ \mathcal{O}_{2,1,1} &= \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}\\ \mathcal{O}_{2,2} &= \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}\\ \mathcal{O}_{3,1} &= \{(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3)\}\\ \mathcal{O}_{4} &= \{(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\}\end{aligned}$$

Now,

$$\begin{aligned}A_4 =&\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),\\ &(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3)\}\end{aligned}$$

Let x be one of $(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g\in A_4\}\\ &= \{(1,2),(3,4),(2,3),(1,3),(2,4),(1,4)\}\end{aligned}$$

Let $x = (1,2,3),(1,3,4),(1,4,2),(2,4,3)$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g\in A_4\}\\ &= \{(1,2,3),(1,3,4),(1,4,2),(2,4,3)\}\end{aligned}$$

Let $x = (1,3,2),(1,2,4),(1,4,3),(2,3,4)$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g\in A_4\}\\ &= \{(1,3,2),(1,4,3),(1,2,4),(2,3,4)\}\end{aligned}$$

Let $x = e$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g \in A_4\} \\ &= \{e\}\end{aligned}$$

Let $x = (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g \in A_4\} \\ &= \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}\end{aligned}$$

Let $x = (1,2,3,4), (1,2,4,3), (1,3,4,2), (1,3,2,4), (1,4,3,2), (1,4,2,3)$

$$\begin{aligned}\mathcal{O}(x) &= \{gxg^{-1} \mid g \in A_4\} \\ &= \{(1,2,3,4), (1,2,4,3), (1,3,2,4), (1,3,4,2), (1,4,2,3), (1,4,3,2)\}\end{aligned}$$

10. Determine all conjugacy classes in D_4, the symmetry group of the square.

Solution:

Let $x = r$

$$\mathcal{O}(x) = \{r, r^3\}$$

Let $x = s$

$$\mathcal{O}(x) = \{s, r^2 s\}$$

Let $x = rs$

$$\mathcal{O}(x) = \{rs, r^3 s\}$$

Let $x = e$

$$\mathcal{O}(x) = \{e\}$$

11. Determine all conjugacy classes in D_5, the symmetry group of the pentagon.

Solution:

$D_5 = \{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$ Let $x = e$

$$\mathcal{O}(x) = \{e\}$$

Let $x = r, r^4$

$$\mathcal{O}(x) = \{r, r^4\}$$

Let $x = r^2, r^3$

$$\mathcal{O}(x) = \{r^2, r^3\}$$

Let $x = s, rs, r^2s, r^3s, r^4s$

$$\mathcal{O}(x) = \{s, rs, r^2s, r^3s, r^4s\}$$

12. Let $O(2,\mathbb{R})$ be the set of 2×2 orthogonal matrices. Describe all of the $O(2,\mathbb{R})$-conjugacy classes.

Solution:

The only two type of elements in $O(2,\mathbb{R})$ are rotations and reflections

$$\begin{aligned} A_\theta &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\ B_\theta &= \begin{pmatrix} -\cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{aligned}$$

So consider conjugating a rotation A_θ by another A_φ

$$A_\varphi A_\theta (A_\varphi)^{-1} = A_\theta$$

conjugating a rotation A_θ by a B_φ

$$B_\varphi A_\theta (B_\varphi)^{-1} = A_{-\theta}$$

Thus

$$\mathcal{A}_\theta = \{A_\theta, A_{-\theta}\}$$

Conjugating reflections with rotations leaves

$$\begin{aligned} A_\theta B_\varphi (A_\theta)^{-1} &= A_\theta B_\varphi A_{-\theta} \\ &= B_\varphi \end{aligned}$$

Thus

$$\mathcal{B}_\varphi = \{B_\varphi\}$$

13. If p is a prime integer, we say a group G is a p-group if every element of G has order p^k for some non-negative k. Prove: A finite group G has order p^n for some $n \geq 0$ if and only if G is a finite p-group. (caution: We do not assume G is abelian.)

Solution:

Proof. $\Longrightarrow$ Let G a finite group, $|G| = p^n, n \geq 0$. Then every element of G must has order p^k for some $k \geq 0$ since order of elements divides order of the group.
$\Longleftarrow$ Let G be a finite p-group. Then every element of G has order p^k for some $k \geq 0$. Assume that $|G| \neq p^n$ for some $n \geq 0$. Then there exists some prime $q \neq p$ such that $q \mid |G|$. Then by Cauchy's Theorem there exists an element with order q, which is a contradiction. Thus $|G| = p^n$ for some $n \geq 0$. □

14. Hungerford: 9.3.2

(a) List three Sylow 2-subgroups of S_4.

Solution:

$$\begin{aligned}
H_1 &= \{e,(1,3),(2,4),(1,3)(2,4),(1,2)(3,4),(1,4)(2,3),(1,2,3,4),(1,4,3,2)\} \\
H_2 &= \{e,(1,4),(2,3),(1,3)(2,4),(1,2)(3,4),(1,4)(2,3),(1,2,4,3),(1,3,4,2)\} \\
H_3 &= \{e,(1,2),(3,4),(1,3)(2,4),(1,2)(3,4),(1,4)(2,3),(1,4,2,3),(1,3,2,4)\}
\end{aligned}$$

(b) List four Sylow 3-subgroups of S_4.

$$\begin{aligned}
H_1 &= \{e,(1,2,3),(1,3,2)\} \\
H_2 &= \{e,(1,2,4),(1,4,2)\} \\
H_3 &= \{e,(1,3,4),(1,4,3)\} \\
H_4 &= \{e,(2,3,4),(2,4,3)\}
\end{aligned}$$

15. Hungerford: 9.3.4
List the Sylow 2-subgroups, Sylow 3-subgroups, and Sylow 5-subgroups of $\mathbb{Z}_{12} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$.

Solution:

$$\begin{aligned}
G &= \mathbb{Z}_{12} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10} \\
|G| &= 12 \cdot 12 \cdot 10 \\
&= 2^5 \cdot 3^2 \cdot 5
\end{aligned}$$

Since $\mathbb{Z}_n, n > 1$ are finite cyclic groups, there is exactly one subgroup of order for each divisor. Thus: The Sylow 2-subgroups has order $2^5 = 32$ and there is only one such subgroup.

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 < G$$

The Sylow 3-subgroups has order $3^2 = 9$ and there is only one such subgroup.

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \{0\}$$

The Sylow 5-subgroups has order 5 and there is only one such subgroup.

$$\{0\} \times \{0\} \times \mathbb{Z}_5$$

University of Washington
Department of Mathematics
MATH 403, Spring 2021

Tuesday 25^{th} May, 2021
Zhewen Zheng

Homework 6

Problems to TURN IN

1. Hungerford: 9.3.18
   If G is a simple group of order 168, how many Sylow 7-subgroups does G have?

   Solution:

   Let n_7 be the number of Sylow 7-subgroups of G. By The Third Sylow Theorem, n_7 must divide 168 and is of the form $n_7 \equiv 1 \mod 7$.

$$\begin{aligned} 168 &= 2^3 \cdot 3 \cdot 7 \\ n_7 &= 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 42, 56, 84, 168 \\ 7 &\mid n_7 - 1 \\ n_7 &= 1, 8 \end{aligned}$$

   If $n_7 = 1$, then there exists a unique Sylow 7-subgroup K, which is normal in G by Corollary 9.16. This is not possible since G is a simple group. Therefore there are $n_7 = 8$ Sylow 7-subgroups in G.

2. Hungerford: 9.3.23

   (a) If $|G| = 105$, prove that G has a subgroup of order 35.

   Proof. Let's take a look at the prime factors of $|G|$. Let n_p stands for number of Sylow p-subgroups.

$$\begin{aligned} 105 &= 3 \cdot 5 \cdot 7 \\ n_5 &= 1, 3, 5, 7, 15, 21, 35, 105 \\ 5 &\mid n_5 - 1 \\ n_5 &= 1, 21 \\ n_7 &= 1, 3, 5, 7, 15, 21, 35, 105 \\ 7 &\mid n_7 - 1 \\ n_7 &= 1, 15 \end{aligned}$$

   Consider that $n_5 = 21$ and $n_7 = 15$. Then each Sylow 5-subgroup there are 4 elements plus the identity, each Sylow 7-subgroup there are 6 elements plus the identity, which gives us $4 \cdot 21 + 6 * 15 = 84 + 90 = 174$ distinct elements. This is impossible, so one of n_5 and n_7 is 1, thus a normal p-subgroup N in G. By the second isomorphism theorem we know that if N, K subgroups of G, N normal in G, then $NK = \{nk \mid n \in N, k \in K\}$ a subgroup of G. Let the normal p-subgroup be N, the other be K. We know that $N \cap K = \{e\}$, thus by Exercise 15

$$|NK| = \frac{|N||K|}{|N \cap K|} = \frac{35}{1} = 35$$

Thus there is a subgroup of order 35 in G. □

(b) If $|G| = 375$, prove that G has a subgroup of order 15.

Proof. Let's take a look at the prime factors of $|G|$. Let n_p stands for number of Sylow p-subgroups.

$$\begin{aligned}
375 &= 3 \cdot 5^3 \\
n_3 &= 1, 3, 5, 15, 25, 75, 125, 375 \\
3 &\mid n_3 - 1 \\
n_3 &= 1, 25 \\
n_5 &= 1, 3, 5, 15, 25, 75, 125, 375 \\
5 &\mid n_5 - 1 \\
n_5 &= 1
\end{aligned}$$

Thus there is a unique Sylow 5-subgroup, which is normal in G. By the second isomorphism theorem we know that if N, K subgroups of G, N normal in G, then $NK = \{nk \mid n \in N, k \in K\}$ a subgroup of G. Let the Sylow 5-subgroup be N, the Sylow 3-subgroup be K. We know that $N \cap K = \{e\}$, thus by Exercise 15

$$|NK| = \frac{|N||K|}{|N \cap K|} = \frac{15}{1} = 15$$

Thus there is a subgroup of order 15 in G. □

3. Hungerford: 9.4.22
If $|G| = p^n$, prove that G has a normal subgroup order p^{n-1}. [Hint: You may assume Theorem 9.27 below. Use induction on n. Let $N = \langle a \rangle$, where $a \in Z(G)$ has order p (Why is there such an a?); then G/N has a subgroup of order p^{n-2}, use Theorem 8.24.]

Solution:

Proof. We do induction on n.
Base Case: $|G| = p^2$, By Theorem 9.27 and Cauchy exists $a \in Z(G), |a| = p$, which gives us $\langle a \rangle$ with order p normal in G.
Induction Hypothesis: If $|G| = p^{n-1}$ then G has a normal subgroup order p^{n-2}.
Inductive Case: By Theorem 9.27 we know that $Z(G)$ is nontrivial. By Cauchy's Theorem there is an element $a \in Z(G)$ such that $|a| = p$. Then take the cyclic subgroup $N = \langle a \rangle$, which is normal in G. By Lagrange, $G/N = \frac{p^n}{p} = p^{n-1}$. By the Induction Hypothesis, there

is an normal subgroup T of G/N with order p^{n-2}. By Theorem 8.24 $T = H/N$ where H is a subgroup of G that contains N. By Lagrange we have

$$\begin{aligned} |H/N| &= \frac{|H|}{|N|} \\ p^{n-2} &= \frac{|H|}{p} \\ |H| &= p^{n-1} \end{aligned}$$

By Corollary 8.23 since $T = H/N$ normal in G/N we have H normal in G.

□

4. Hungerford: 9.5.2
   Prove that there is no simple group of order 12, [Hint: Show that one of the Sylow subgroups must be normal.]

   Solution:

   Proof. Let G be a group of order 12. Let's take a look at the prime factors of $|G|$. Let n_p stands for number of Sylow p-subgroups.

$$\begin{aligned} n_2 &= 1, 2, 3, 4, 6, 12 \\ 2 &\mid n_2 - 1 \\ n_2 &= 1, 3 \\ n_3 &= 1, 2, 3, 4, 6, 12 \\ 3 &\mid n_3 - 1 \\ n_3 &= 1, 4 \end{aligned}$$

   Suppose $n_3 = 4$. Then there would be $4 \cdot (3 - 1) = 8$ distinct nontrivial elements from the Sylow 3-subgroups. Now by the First Sylow Theorem we are guaranteed a Sylow 2-subgroup of order $2^2 = 4$. This implies all elements of G has already been taken and Sylow 2-subgroup was unique and normal. If $n_3 = 1$ then the Sylow 3-subgroup was normal. In either cases, there exists a normal subgroup of G where G has order 12. Thus G must not be simple. □

5. Prove: No group of order p^2q^2 is simple when p and q are primes.

   Solution:

   Proof. Let G be a group of order p^2q^2, p, q primes. WLOG let $p < q$. Let's see the possible number of Sylow q-subgroups:

$$\begin{aligned} n_q \mid |G|, q \mid n_q - 1 \\ n_q = 1, p^2 \\ q \mid p^2 - 1 \implies q \mid (p-1) \text{ or } q \mid (p+1) \end{aligned}$$

if $n_3 = 1$ we are clear(unique proper Sylow q-subgroup which is normal in G). If there are more than one Sylow q-subgroups, we must satisfy $q \mid (p+1)$ since $p < q$. Since p, q primes, the only possible case is $p = 2, q = 3$. This means we need to show $|G| = 36$ is not simple. Let $|G| = 2^2 3^2 = 36$. Assume that $n_3 = 2^2 = 4$. Let $X = \{H_1, H_2, H_3, H_4\}$ where H_i are the set of four Sylow-3 subgroups in G.
Consider G act on X by conjugation. We would obtain a homomorphism

$$\varphi : G \to S(X), S(X) \cong S_4$$
$$\varphi_g(x) = g^{-1}hg$$

Clearly the function is not injective since $|G| = 36, |S_4| = 24$. Thus the Kernel must be nontrivial. By the Second Sylow Theorem K must not be G either. Therefore there exists a normal subgroup K of G. Therefore no group of order p^2q^2 is simple for p, q primes. □

6. Let $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{q^2}$ where $p < q$ are primes.

   (a) Explain why there is a unique subgroup of order p^2 and a unique subgroup of order q^2.

   Solution:

   The First Sylow Theorem guarantees the existence of a subgroup of order p^2 and a subgroup of order q^2. Now since G is a finite abelian group, the subgroups are abelian and thus normal. Then by Corollary 9.16 we know that they are unique in G.

   (b) Explain why there is not a unique subgroup of order p.

   Solution:

   Consider $\langle a, 0, 0\rangle$ and $\langle 0, a, 0\rangle$. Clearly both are cyclic subgroups of order p and different.

   (c) Is there a unique subgroup of order q? Explain?

   Solution:

   By The First Sylow Theorem we know that there is subgroups of order q and order q^2. p is prime and $p < q$ so The choice from $\mathbb{Z}_p$ is locked to the identity 0. Since $\mathbb{Z}_{q^2}$ is a finite abelian group we know that there is a unique subgroup of order q of $\mathbb{Z}_{q^2}$. Thus our unique subgroup of order q of G is $\langle (0, 0, q)\rangle$.

7. Suppose a finite group G acts on a finite set X. Prove: If g and h are conjugate in G, then $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$. In other words, conjugate elements fix the same number of points.

   Solution:

   Proof. Let $g = s^{-1}hs, g, h, s \in G, x \in \operatorname{Fix}(g)$. Then

$$\begin{aligned} gx &= x \\ (s^{-1}hs)x &= x \\ s^{-1}(hs)(x) &= x \\ h(sx) &= sx, sx \in \operatorname{Fix}(h) \end{aligned}$$

Let $f : \operatorname{Fix}(g) \to \operatorname{Fix}(h), f(x) = sx$. This is well-defined as seen above.
Injective: Let $x_1, x_2 \in \operatorname{Fix}(g), f(x_1) = f(x_2)$

$$\begin{aligned} f(x_1) &= f(x_2) \\ sx_1 &= sx_2 \\ x_1 &= x_2 \end{aligned}$$

Thus f is injective.
Surjective: Let $y \in \operatorname{Fix}(h)$. Then we have

$$\begin{aligned} x &= s^{-1}y \\ f(x) &= sx \\ &= ss^{-1}y \\ &= y \in \operatorname{Fix}(h) \end{aligned}$$

Thus f is surjective. Therefore f is bijective and hence $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$ for conjugates $g, h \in G$. □

8. Suppose we want to color the faces of a cube using either red or green paint. Use the "Counting Theorem" in Lecture 24 and the description of the rotational symmetry group of the cube in Lecture 25 to determine the total number of genuinely different painted cubes you can obtain. (Note: If you were to paint the top red and all other faces green, we consider that the same coloring as if we had painted the bottom red and all other faces green, since an obvious rotational symmetry takes one coloring to the other.)

Solution:

The Counting Theorem states that

$$\text{number of orbits in } G = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$$

In lecture 25 we have considered $X = \{N_1, N_2, N_3, N_4\}$ where N_i are the four diagonals that crosses the origin. The group acting on X is $G = S_4$, as we see that

$$\begin{aligned} &r : \text{rotate } \frac{\pi}{2} \text{ counterclockwise around } L = (1234) \\ &s : \text{rotate } \frac{2\pi}{3} \text{ counterclockwise around } N = (143) \\ &t : \text{rotate } \pi \text{ counterclockwise around } M = (1234) = (12) \end{aligned}$$

with $\varphi : G \to S_4$ is a bijection since $|G| = 24 = |S_4|$ and $S_4 = \langle (1234), (12) \rangle$. We also know the conjugacy classes of S_4:

Partition Type	elements	Conjugacy Class
$1, 1, 1, 1$	$\{()\}$	$\mathcal{C}_e$
$2, 1, 1$	$\{(12), (13), (14), (23), (24), (34)\}$	$\mathcal{C}_{(12)}$
$3, 1$	$\{(123), (132), (124), (142), (134), (143), (234), (243)\}$	$\mathcal{C}_{(123)}$
4	$\{(1234), (1243), (1324), (1342), (1423), (1432)\}$	$\mathcal{C}_{(1234)}$

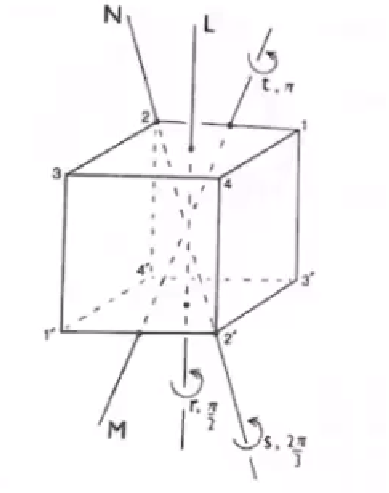

Figure 11: Rotational Symmetries of the Cube

Now we check the fix cases for a representative of each conjugacy class:

Conjugacy Class	$\lvert \mathrm{Fix}(g) \rvert$
$\mathcal{C}_e$	64
$\mathcal{C}_{(12)}$	8
$\mathcal{C}_{(143)}$	4
$\mathcal{C}_{(13)(24)}$	16
$\mathcal{C}_{(1234)}$	8

So

$$\begin{aligned}\text{number of orbits} &= \frac{1}{|G|}\sum_{g\in S_4} \lvert \mathrm{Fix}(g) \rvert \\ &= \frac{1}{24}(64 + (6\cdot 8) + (8\cdot 4) + (3\cdot 16) + (6\cdot 8)) \\ &= \frac{240}{24} \\ &= 10\end{aligned}$$

9. How many different necklaces of 9 beads can you make if you have three different colors of beads to use? Solve this using the ideas from Lecture 24.

Solution:

Let

$$X = \{3^9 = 19683 \text{ arrangements of necklaces of 9 beads}\}$$

. Let $G = D_9$, which will act on X obviously. We want the number of D_9 orbits in X.

$$\text{number of orbits in } G = \frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}(g)|$$

We know that

$$D_9 = \{e, r, r^2, \cdots, r^8, d, rd, r^2d, \cdots, r^8d\}, |D_9| = 2 \cdot 9 = 18$$

Conjugacy Class	elements
$\mathcal{C}_e$	$\{e\}$
$\mathcal{C}_r$	$\{r, r^8\}$
$\mathcal{C}_{r^2}$	$\{r^2, r^7\}$
$\mathcal{C}_{r^3}$	$\{r^3, r^6\}$
$\mathcal{C}_{r^4}$	$\{r^4, r^5\}$
$\mathcal{C}_d$	$\{d, rd, r^2d, r^3d, r^4d, r^5d, r^6d, r^7d, r^8d\}$

Now we check the fix cases for a representative of each conjugacy class:

Conjugacy Class	Fix(g)	$\lvert\operatorname{Fix}(g)\rvert$
$\mathcal{C}_e$	Fix(e)	$3^9 = 19683$
$\mathcal{C}_r$	Fix(r)	3
$\mathcal{C}_{r^2}$	Fix(r^2)	3
$\mathcal{C}_{r^3}$	Fix(r^3)	27
$\mathcal{C}_{r^4}$	Fix(r^4)	3
$\mathcal{C}_d$	Fix(d)	8

Thus

$$\text{number of orbits in } G = \frac{1}{18}(19683 + 2 \cdot 3 + 2 \cdot 3 + 2 \cdot 27 + 2 \cdot 3 + 9 \cdot 243) = 1219$$

there are 1219 distinct 9 beads 3 color necklaces.